UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA - v. - PIERRE GIRGIS, Defendant.	22 Cr. 6 (KPF)

GOVERNMENT'S MEMORANDUM OF LAW
IN OPPOSITION TO DEFENDANT'S MOTIONS TO COMPEL

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York
One St. Andrew's Plaza
New York, NY 10007

Kyle A. Wirshba
Elinor L. Tarlow
Sarah L. Kushner
Assistant United States Attorneys
-Of Counsel-

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes

Rules

PRELIMINARY STATEMENT

The Government respectfully submits this memorandum in opposition to defendant Pierre Girgis's Motion to Compel. *See* Dkt. 36 ("Mot."). Girgis seeks to compel production of (i) any Foreign Intelligence Surveillance Act ("FISA") applications, warrants, and materials related to this case, *see* 50 U.S.C. §§ 1801 *et seq.*; (ii) notice of any non-FISA surveillance methods used by the Government to surveil his communications and personal information; (iii) further information about an affidavit for a warrant issued pursuant to Federal Rule of Criminal Procedure 41; (iv) information about nine Egyptian officials who interacted with Girgis; and (v) information about the role if any that a particular former Federal Bureau of Investigation ("FBI") official played in the investigation into Girgis. For the reasons that follow, these motions are meritless and the Court should deny Girgis's requested relief.

Girgis is a dual American and Egyptian citizen who emigrated to the United States from Egypt in 2009 and settled in the New York City area. In approximately 2014, Girgis began acting in the United States as an agent of Egypt, including by working on behalf of Egyptian diplomats stationed in New York and several officers of the Administrative Control Authority ("ACA"), an Egyptian law enforcement body that also engages in intelligence gathering activities. In the years since, and as described in more detail below, Girgis has, under the direction and control of Egyptian officials, worked to further Egyptian interests in connection with U.S. law enforcement by, among other things: tracking anti-Egyptian government protesters and encouraging U.S. law enforcement to prosecute them; requesting and obtaining non-public information from U.S. law enforcement about political enemies of Egypt's president; arranging Egyptian dignitaries' travel in the United States; and coordinating meetings between Egyptian and U.S. law enforcement.

Girgis's motions should be denied. Regarding his motion to compel any FISA applications, warrants, or other materials and his request for notice of any additional classified surveillance techniques used in this case, the Government explains the reasons requiring denial of Girgis's motion in a classified, *ex parte* supplement to this memorandum (the "Classified Supplement"), a redacted unclassified version of which is attached hereto as Exhibit A, along with a declaration of the Attorney General, which is attached hereto as Exhibit B.

Girgis's additional motions should also be rejected. He moves to compel the production of information about the Government's application in this case for a warrant pursuant to Rule 41, which he claims he needs in support of his anticipated motion under *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978), and which he argues the Government must provide under *Giglio v. United States*, 405 U.S. 150, 154 (1972). The Government has already provided information related to the Rule 41 warrant application, including witness statements, and understands its continuing obligation to provide additional materials, if identified, relevant to Girgis's potential *Franks* motion.

Girgis's motion seeking additional information regarding nine Egyptian officials is equally unavailing. The Government has already provided relevant information documenting those officials' interactions with Girgis, and the efforts of Egyptian officials to direct and control individuals other than Girgis are not relevant to the issues that are properly the subject of litigation in this matter and are not otherwise discoverable.

Finally, Girgis's motion for information about the role of a former FBI official should also be denied. Girgis does not identify any basis for discoverability of such material, nor is the Government aware of any discoverable information.

BACKGROUND

I. Factual Summary

A. Girgis Develops Relationships with Egyptian Officials

As early as 2014, Girgis was communicating regularly via encrypted applications with multiple Egyptian officials discussing, among other things, protests against Egyptian President Abdel-Fattah el-Sisi, how Girgis might leverage contacts he had at the New York City Police Department ("NYPD") to further Egyptian interests, and travel arrangements for incoming Egyptian officials.

On January 18, 2016, for example, Girgis exchanged messages with Mohamed Ramadan ("Ramadan"), an Egyptian official employed at the Egyptian Consulate in Manhattan. Girgis stored Ramadan's number in his phone as "Mohamed Ramdan Consulate." Girgis and Ramadan discussed Girgis's NYPD contacts, pro-Egyptian government events at the Egyptian Consulate in Manhattan, and New York-based critics of Egyptian President el-Sisi.

By late 2016, Girgis was coordinating travel for incoming Egyptian dignitaries at the request and the direction of Ezzat Mokhtar Farag Morsy ("Mokhtar"), an Egyptian ACA officer, whose contact information is saved in Girgis's phone as "Ezzat VIP." On November 30, 2016, Mokhtar asked Girgis, via an encrypted messaging application, to complete "a big favor" for "an extreme[ly] important family" that would be visiting New York from Egypt. Mokhtar directed Girgis to "find a very secure villa" with four rooms in New Jersey for particular dates in December and January, stressing that "no one is to know anything." After receiving this request, Girgis booked an Airbnb in New Jersey on the dates Mokhtar had directed and paid using his own American Express card, later receiving email confirmation. On those dates, family members of Egyptian President el-Sisi arrived in and then left New York.

B. Girgis Monitors and Investigates Opponents of the Egyptian Government as Part of His Work for Egyptian Officials

By late 2016, Girgis was monitoring—both on social media and in person—anti-Sisi protest activity by a group of activists and reporting their activities to Egyptian officials. Based on their encrypted communications, the Egyptian officials directing Girgis were particularly focused on two New York-based Egyptian anti-Sisi activists ("Activist-1" and "Activist-2"), regularly exchanging messages about the activities of Activist-1 and Activist-2, as well as a protest group in which they both belonged based on social media ("Protest Group-1").

On March 31, 2017, for example, Protest Group-1 posted on Facebook a flyer for an April 3, 2017 protest in Washington, D.C. against el-Sisi's upcoming visit to the White House. On April 1, 2017, Ramadan sent Girgis a link to a video that Activist-2 had posted of himself on Facebook. In response, Girgis wrote, "encouraging violence on US soil. I have contacted our beloveds and they are working on him," an apparent reference to Girgis's contacts in the NYPD, with whom Girgis communicated before and after the el-Sisi protest. Girgis also received messages about the upcoming protests from Mohamed Hassan Elsayed ("Elsayed"), an Egyptian official working at the Egyptian Mission to the United Nations in New York. Girgis stored Elsayed's number in his phone as "Mohamed Hassan Egyptian Mission." On April 2, 2017, the day before the el-Sisi White House visit, Elsayed messaged Girgis via encrypted application, sending several photographs of Activist-1 and Activist-2 together on a bus destined for Washington, D.C.

On April 3, 2017, the day of the White House visit, Girgis traveled to Washington, D.C., where he monitored the protests in person. During the protests, violence broke out. As reported in public press, anti-Sisi protesters assaulted a well-known Egyptian media personality who was part of el-Sisi's media delegation to the United States. The perpetrators were arrested by the

Washington, D.C. Metropolitan Police Department.[1] In the aftermath of this assault, Girgis received information from Egyptian officials and passed the information to Girgis's NYPD contacts, in an effort to prompt the NYPD to take action against the assailants. For example, Girgis received photographs and videos of the assailants from Ramadan and Elsayed, which had been mined from both preexisting social media and photographs from the assault, and sent that information to multiple members of the NYPD.

C. Girgis Requests That NYPD Officers Obtain Non-Public Information for Egyptian Officials

On at least three separate occasions following this trip to Washington, D.C. to monitor and report to Egyptian officials on the anti-Sisi protests, Girgis requested non-public information from NYPD officers concerning individuals of interest to Egyptian government officials.

On April 8, 2017—approximately one week after the assault and arrests in Washington, D.C.—Girgis sent two phone numbers to Ramadan, and then a half hour later sent the same numbers to a particular NYPD officer ("Officer-1") followed by the message, "Ramdan." Officer-1 responded "ok." On the next day, April 9, 2017, Ramadan sent Girgis what appears to be a still from a security camera showing an unknown individual on the street, which Girgis promptly forwarded to Officer-1. Officer-1, responding to Girgis's message from the prior day providing the two phone numbers, wrote, "both numbers are fake." Girgis responded, "thanks for looking into it. hope nothing bad happen here." Officer-1 assured him, "nothing gonna happen."

Girgis next requested non-public information from the NYPD in September 2017. On September 8, 2017, Activist-1 posted on Facebook a flyer for a "huge protest against Sisi's visit

---

[1] *See* https://pressfreedomtracker.us/all-incidents/egyptian-talk-show-host-slapped-back-neck/; https://english.alaraby.co.uk/english/news/2017/4/4/egypt-journalist-attacked-by-anti-sisi-protesters-in-washington-streets.

to the United Nations." Three days later, on September 11, 2017, Girgis sent Officer-1 an encrypted message containing a screenshot of Activist-1's Facebook post with the flyer, which also indicated that Activist-1 would attend the event. Officer-1 responded, "already handled," to which Girgis replied, "Can you tell me what steps you to[o]k? The dep I mean," referring to the "department," *i.e.*, NYPD. In response, Officer-1 wrote, "when we talk." The next day, on September 12, 2017, Girgis asked Officer-1, via encrypted message, for a list, to which Officer-1 responded, "What list?" and Girgis clarified, "protesters list." Officer-1 wrote to Girgis, "I don't think they will give it to us."

Girgis made a third request for non-public information from NYPD on November 28, 2017. That day, Elsayed sent Girgis a picture of a photo identification card of a particular Egyptian national ("Egyptian-1"). According to NYPD records, on November 22, 2017, Egyptian-1 had been arrested for touching multiple victims' buttocks without permission on a Manhattan street. On November 28, 2017—the day of Elsayed's message—Egyptian-1 was released. Upon receiving the identification card, Girgis promptly forwarded it by encrypted message to Officer-1 and three other NYPD officers ("Officer-2," "Officer-3," and "Officer-4"). Approximately two hours later, Officer-1 responded, "Thank u." Officer-2 responded, "I need a date of birth on him," to which Girgis responded, "i know he lives in queens," prompting Officer-2 to reply, "Without it I can't." Girgis, upon receiving Officer-2's response, messaged Elsayed, "Mohamed i need his date of birth," to which Elsayed replied, "I'll try to get it." Officer-4 replied, "Do u have date of birth" and, according to NYPD records, searched at least one NYPD database for Egyptian-1's name. Officer-4 later responded to Girgis, "Can't find anything in the system[.] Give an address or DOB."

D. Girgis Arranges for an April 2018 Visit by ACA Officials

In April 2018, in coordination with Egyptian officials, Girgis planned a visit for four ACA officials to the United States. For example, on April 14, 2018, Girgis asked Mokhtar to "send me the passports of you [and] the group [c]oming god willing on the 27." In response, Mokhtar sent pictures of three passports: his own; that of Ahmed Mostafa Ahmed Elbehiry ("Elbehiry"), which listed that Elbehiry was employed as an ACA officer; and that of Mohamed Mohamed Efran Gamaleldim ("Gamaleldim"), which listed that Gamaleldim was employed as the Chairman of the ACA. Girgis discussed with Mokhtar, via encrypted messages, different hotel options for the three visiting ACA officials and ultimately paid for Mokhtar's hotel room.

During this April 2018 trip, Girgis also acted on behalf of Mokhtar to arrange transportation, through the NYPD, for the visiting Egyptian officials. On April 21, 2018, Girgis exchanged text messages with an NYPD Deputy Inspector ("Inspector-1"). Girgis texted Inspector-1 about securing a police escort for the ACA officials from JFK Airport to the midtown hotel where the officials would be staying. On April 25, 2018, Inspector-1 confirmed that the "chief said he can assign couple detectives" but that he needed "a point of contact and list of all names . . . ASAP." Girgis sent screenshots of his conversation with Inspector-1 to Mokhtar, stating, "Ezzat plz provide me this info asap can't wait till tomorrow I'm having the whole nypd." Approximately two hours later, Girgis sent Inspector-1 the list of ACA officials who would be arriving as well as their flight information.

On April 26, 2018, Girgis wrote Inspector-1 informing him that Girgis had received a call from an NYPD sergeant who said NYPD planned to send two detectives to escort the officials the next day. In response, Inspector-1 wrote to Girgis, "you coordinate with them and advise if any issues."

E. Mokhtar Confirms Girgis's Status as an Egyptian Agent Working at ACA's Direction

Girgis and Mokhtar also expressly discussed Girgis's value to the ACA as its agent. In particular, in an encrypted messaging exchange between Girgis and Mokhtar on May 7, 2018, Mokhtar wrote Girgis in apparent anger over Girgis's recent contact with an Egyptian intelligence service (*i.e.*, a different branch of the Egyptian government than the ACA). In the messages, excerpted below, Mokhtar confirmed that Girgis was a source belonging to the ACA whose assistance to the ACA had been reported to government officials in Egypt, prompting Girgis to repeatedly apologize for his perceived lack of loyalty and to reaffirm his commitment to serving Mokhtar and the ACA.

Girgis: Can I call you?

Mokhtar: We have our own secrets, and I had warned you. This is the biggest mistake Pierre, as it is not possible to open with all the agencies. I'm letting you open with us only. Everything I have stated has been written and sent to Egypt. All this talk has been written and sent to Egypt . . . . Seriously, you are humiliating me, you have no idea what can happen. This way the good things you do, you ruin in a second. I'm the one to be humiliated because you do not listen to my words. . . . I had warned you, and you insist on opening with the Mukhabarat.[2] This way you are hurting me . . . . Really I'm very, very sad. Because you do a lot of good things, but you ruin them in a second, not just that, you are also hurting me

. . .

Girgis: I'm sorry

Mokhtar: You don't listen to me. He asked you and tricked you because he wanted to send it, and you fell and let him know. Pierre you supposed to say, I don't know, I did not do. You hurt me Pierre.

Girgis: I'm sorry, the last thing I do is to hurt you, I will pull out quietly

. . .

[2] "Mukhabarat" is the generic Arabic word used for intelligence agencies.

Mokhtar: I do for you this and that. They want sources for themselves, and you have become an important source for them to collect information. I had warned you.

Girgis: I know and I see and I learn from you. But I don't understand who wants, uhh and when he asked me if he can send a letter I understood that he wants to help.

Mokhtar: Now you have seen, I hope, I hope you learn.

Girgis: But it will not be repeated again.

In this conversation, Mokhtar confirmed that Girgis was serving as a source for the ACA ("you do a lot of good things"), and emphasized that Girgis could only act pursuant to the ACA's commands ("I'm letting you open with us only"), and Girgis reaffirmed that he would act only under the ACA's direction and control and not again contact the other Egyptian intelligence service ("it will not be repeated again").

F. Girgis Applies to FBI at the Direction of Egyptian Officials

In 2017, Girgis applied to become a special agent at FBI at the direction of Egyptian officials. Recognizing that an apparent agent of a foreign power was attempting to join its ranks, FBI closely monitored and documented Girgis's participation in the process. As part of that application process, Girgis participated in an FBI "meet and greet" and attended an in-person interview. Ultimately, FBI did not offer Girgis a position. Nonetheless, on June 22, 2018, Girgis called an FBI application coordinator to follow up. During the call, Girgis expressed his disappointment that FBI did not hire him and claimed that he was interested in assisting FBI.

In response to Girgis's purported offer to assist FBI, on February 26, 2019, an FBI agent called Girgis and offered to meet. Girgis accepted. On February 28, 2019, FBI agents met with Girgis for a voluntary, recorded interview at FBI offices in Manhattan. During the meeting, in substance and in part, Girgis said that he was close to members of the ACA, which Girgis characterized as an Egyptian government law enforcement agency responsible for anti-corruption

and counterterrorism, among other things. Girgis told the agents that in his free time, he had organized a trip to Egypt for law enforcement officers in March 2018. Girgis said that a number of NYPD officers, among other law enforcement officers, attended the trip. Girgis explained that the ACA significantly supported the trip with security and special privileges, providing as an example that in order to get all the visas processed in time for the trip, the Egyptian Consulate stayed open after normal hours as a favor to Girgis. Girgis also offered to introduce the interviewing FBI agents to ACA officials who would be visiting the United States in March 2019. Girgis further expressed concern about a Muslim protest organization that operated in New York City, including its connection to the Muslim Brotherhood, an anti-Sisi party in Egypt. Girgis said that one of the ACA officials had encouraged him to apply for the job at FBI.

G. Girgis Arranges a Meeting Between Egyptian ACA Officials and NYPD Leadership

As part of his service to ACA and efforts to further Egyptian interests in the United States, Girgis worked to arrange a meeting between ACA officials and U.S. law enforcement in early 2019. In preparation for these meetings, Mokhtar gave Girgis explicit instructions on what he should be doing to coordinate those meetings. During a call on March 8, 2019, an excerpt from a draft transcript of which is below, Mokhtar directed Girgis as follows:

Girgis:	Tell me what you want me to do.
Mokhtar:	You relationship with him is very good?
Girgis:	My relationship? With whom, with [Inspector-1]? I have very good relationship with [Inspector-1].
Mokhtar:	We want to you to ask him for something. We want you to find out if there are any police training/meeting happening in Manhattan in the coming days, and if so, who are the people in charge of these trainings? We would like to attend.
Girgis:	You told me don’t push?

Mokhtar: I told you I would talk to you first. If not, I will talk to [another NYPD officer ("Officer-5")] and see if he could get us an appointment with his man.

Girgis: Don't talk to [Officer-5] because I already talked to his man

Mokhtar: What did the man tell you?

Girgis: When I met them in March, he told me neither him nor the NYPD Commissioner would be available during this time. I will reach back out to the Lieutenant whom I spoke with.

Mokhtar: We want to come to see what arrangements they have, or what kind of cooperation they offer us these days.

Girgis: So, shall I start talking to the Lieutenant again?

Mokhtar: Yes. Talk.

Girgis: I don't want to mix things together though, because if you talk to [Officer-5], things will get messed up.

Mokhtar: That is why I am asking you now.

Girgis: I already met and spoke with [Officer-5]'s manager.

Mokhtar: [Officer-5] asked me if we need anything from them, that is why I asked you what you are going to do?

Girgis: What you want me to do? I told them that I met with the [Officer-5]'s top manager, the chief of the whole unit. . . . I went in, we sat together, I gave him the things, I told him about you and sent him the information.

Mokhtar: Make follow up, Ok?

Girgis: Ok.

In this conversation, Girgis explicitly requested instructions from Mokhtar ("tell me what you want me to do"), referred to prior instructions that Mokhtar had given to him ("you told me don't push"), received a new task from Mokhtar ("make follow up ok"), and agreed to engage in that conduct at the direction of Mokhtar ("ok").

As instructed, Girgis then arranged the meeting, exchanging multiple emails with NYPD officials. On March 15, 2019, Girgis attended the meeting he had arranged at the NYPD, which involved ACA officials and high-level NYPD officials, as well as—unbeknownst to Girgis—an FBI employee. Representing the ACA were Mokhtar, who identified himself as Chief of Staff of the ACA; Mohamed Elngomy, who identified himself as an ACA investigations group leader; and a third ACA official, who identified himself as the head of secret service of the ACA. During the meeting, Girgis acted as a translator for the ACA officials, who discussed collaborating with the NYPD. The NYPD officials, having been made aware by FBI of its investigation into Girgis's activities, agreed that collaboration was important but said that further requests for information or collaborative meetings had to be officially requested through the NYPD's External Affairs office.

H. Girgis Pushes the NYPD to Prosecute Activist-2

In April 2019, as Girgis and his Egyptian handlers continued their efforts to disrupt lawful protest activities, Girgis acted as an intermediary between Egyptian officials and another NYPD officer ("Officer-6") to further an investigation into Activist-2.

During an exchange of encrypted messages with Officer-6, Officer-6 provided Girgis with Activist-2's bank account number, phone number, and bank account activity, and asked Girgis to "keep it confidential." Girgis passed this information to Egyptian officials Ramadan and Elbehiry. During the exchange, Girgis also made suggestions to Officer-6 about how Activist-2 could be criminally charged, such as "by any chance can you check if he is on Medicaid or if he's taking welfare . . . you should it will help your investigation. charge of committing fraud by submitting false statements." Officer-6 later wrote, "I don't know how u going to get info, but if u can try not to mention it's law enforcement related. But most important I want to know who is he sending money to in Egypt." Girgis responded, "no worries. I will get you the info soon." Later that

evening, Girgis asked Ramadan, "if you have pictures with [Activist-1] and [Activist-2] or any of the people you know plz send it to me. I want them to link a relate everyone," indicating an effort by Girgis to influence Officer-6's investigation and expand the targeting to include as many anti-Sisi protesters as possible. Several days later, Elbehiry sent to Girgis encrypted messages with the full names of Activist-2 and his wife, along with an "id#" for Activist-2, which Girgis forwarded to Officer-6. Girgis did not succeed in having charges filed against Activist-2.

II. The Government's Investigation and Charges

The investigation of Girgis and his co-conspirators involved, among other things, the collection of records through numerous grand jury subpoenas; the use of FBI confidential sources; witness interviews; the collection of records from other government agencies; and other investigative methods.[3] In addition, the Government obtained search warrants, pursuant to Federal Rule of Criminal Procedure 41 and the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, based on a single affidavit. In particular, on October 25, 2019, the Honorable Vera M. Scanlon, United States Magistrate Judge for the Eastern District of New York, authorized a search for information associated with Girgis's Yahoo email account, information associated with his Apple iCloud account, and any electronic devices found on his person or in his personal effects, based on an affidavit by FBI Special Agent Brian Connors (the "Rule 41 Affidavit"). *See* Mot. Ex. B.

The Rule 41 Affidavit described, among other things, the evidence gathered from Girgis's application and interview with FBI, his interactions with NYPD officials when coordinating a

[3] The Government has provided Girgis with notice of its intent to offer into evidence, or otherwise use or disclose in any proceedings in this matter, information obtained or derived from electronic surveillance and physical search conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. §§ 1801-1812. Further information regarding aspects of these matters pertaining to Girgis's pretrial motions is set forth in the Classified Supplement, which, for the reasons set forth therein, is appropriately submitted *ex parte*.

meeting between the NYPD and ACA, and an order pursuant to 18 U.S.C. § 2703(d). In particular, the Rule 41 Affidavit includes several paragraphs detailing Girgis's description of his Egyptian contacts to FBI as part of his "application" to work for FBI. These include Girgis's recorded statements to FBI, in sum and substance: (i) that he was close to members of the ACA, *see* Mot. Ex. B ¶ 23(a); (ii) that he could introduce FBI agents to ACA members, whom he identified by name, *see id*. ¶¶ 23(a), (f); (iii) that one ACA official had encouraged him to apply for the job at FBI, *see id*. ¶ 23(f); (iv) that he had organized a trip to Egypt for law enforcement officers in March 2018, *see id*. ¶ 23(b); (v) that the "[t]he ACA significantly supported the trip with security and special privileges," *id*.; (vi) that to facilitate the trip, the Egyptian Consulate had processed all necessary visas and stayed open after normal hours as a favor to Girgis, *see id*.; and (vii) that he had taken a video inside a mosque in which he suspected an organization supporting the Muslim Brotherhood was being operated, *see id*. ¶¶ 23(d)-(e). The Rule 41 Affidavit also describes in detail: (i) Girgis's emails to NYPD officers copying several ACA officials seeking to "facilitate a meeting . . . [t]he purpose [of which is] to build a bridge among both agency to better collaborate in the future," *see id*. ¶ 26(h); (ii) other emails coordinating an exact time and place for the meeting, *see id*. ¶¶ 26(i)-(l); (iii) Girgis's email providing the names and titles of the attending ACA officials, *see id*. ¶ 26(k); (iv) travel records indicating that the ACA officials lied about their addresses in New York, and the significance of those lies to Special Agent Connors, which, based on his training and experience, indicated an attempt to thwart FBI surveillance of ACA activities in the United States, *see id*. ¶ 26(m); and (v) what transpired during the meeting between ACA and NYPD officials, as set forth below:

> On or about March 15, 2019, GIRGIS and three ACA officials, including ACA Official-1,[4] attended a meeting at the NYPD with the NYPD Intelligence Official, the NYPD Lieutenant, and other NYPD officials. During the meeting, GIRGIS and ACA Official-1 acted as Arabic translators for the other ACA officials, and GIRGIS translated the ACA officials' comments from Arabic to English for the NYPD officials. The NYPD officials introduced themselves and briefly discussed their various departments and responsibilities. GIRGIS asked why the NYPD did not have an office in Egypt. The NYPD officials explained that their foreign offices were regional rather than specific to individual countries, and that the NYPD's office in Jordan covered northern Africa. Among other things, the ACA officials described the ACA's work in Egypt, including anti-corruption and counterterrorism investigations. One of the ACA officials said that the ACA knew that New York had a large Egyptian population, and that working with the NYPD would help the ACA with the ACA's active investigations of members of the Egyptian émigré community. The NYPD officials agreed that collaboration was important but said that further requests for information or collaborative meetings had to be officially requested through the NYPD's External Affairs office. At the end of the meeting, the NYPD officials took photographs with the ACA officials. GIRGIS initially declined to take part in the group picture-taking but later agreed to be in a group photograph.

See id. ¶ 26(o). The Rule 41 Affidavit further detailed returns from an order obtained pursuant to 18 U.S.C. § 2703(d) indicating that Girgis communicated on nine occasions since 2015 with an apparent Egyptian official who was using the email address "'egyptcg@aol.com,' which appeared to be saved in [Girgis's] contacts as 'Consulate General of Egypt in New York.'" *See id.* ¶ 35.

The Rule 41 Affidavit also described evidence provided by a retired law enforcement officer, referred to as "Retired Captain-1," including that (i) Girgis coordinated several trips to Egypt for U.S. law enforcement, *see id.* ¶¶ 17, 27; (ii) Retired Captain-1 understood the purpose of the 2018 Egypt trip was to "promot[e] Egypt's image among U.S. law enforcement officers"

---

[4] The Rule 41 Affidavit referred to Mohamed Elngomy, who identified himself in a meeting with NYPD as an ACA investigations group leader, *see supra* 12, as "ACA Official-1."

and Retired Captain-1 believed that Girgis "may have been working for or on behalf of the Egyptian Government in organizing and executing the 2018 Egypt trip," *see id.* ¶ 17(g); (iii) Girgis informed Retired Captain-1 that Egyptian officials, on multiple occasions, had requested Girgis's assistance in arranging meetings with NYPD officials, *see id.* ¶ 26(f); and (iv) at Girgis's request, Retired Captain-1 coordinated and attended at least one meeting with certain ACA officials, *see id.* ¶ 26(p).

In the Rule 41 Affidavit, a footnote describing Retired Captain-1 stated:

> In or about August 2018, other FBI agents and I first interviewed Retired Captain-1 regarding his interactions with and knowledge of GIRGIS. Retired Captain-1 agreed to assist FBI in its investigation of GIRGIS. Since in or about August 2018, Retired Captain-1 has been communicating and meeting with GIRGIS at FBI's direction[.]

Id. at 9 n.1. The Rule 41 Affidavit did not reference the fact that Retired Captain-1 had been convicted in New York State court for official misconduct of a public servant performing an illegal function, a class A misdemeanor, a fact not known to Special Agent Connors at the time the warrant was sworn (but learned after the fact and disclosed to the defense, *see* Mot. Ex. A). The Rule 41 Affidavit did, however, include various forms of corroboration for Retired Captain-1's statements, including a group text message chain in which Girgis and Retired Captain-1 participated and in which they coordinated trips to Egypt, *see* Mot. Ex. B ¶¶ 17(c), 26(d); emails from Girgis to Retired Captain-1 discussing those trips and arranging meetings with Egyptian officials, *see id.* ¶¶ 17(c), 26(f)-(g), 26(q)-(s); and photographs taken by Retired Captain-1 during his meeting with ACA officials that FBI had reviewed, *see id.* ¶ 26(n).

Pursuant to the warrants issued based on the Rule 41 Affidavit, FBI conducted a search of, among other things, Girgis and the electronic devices found on his person. On Girgis's primary cellphone, the Government found thousands of encrypted messages with Egyptian officials over

multiple encrypted messaging platforms, some of which are described above. The Government understands that the defense likely will move to suppress those warrants, pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). *See* Mot. at 34 (noting a "forthcoming *Franks* motion").

On January 5, 2022, a grand jury in this District returned an indictment charging Girgis with conspiring to act as an agent of Egypt without prior notification to the Attorney General, in violation of Title 18, United States Code, Section 371 (Count One), and with acting and attempting to act as an agent of Egypt, without prior notification to the Attorney General, in violation of Title 18, United States Code, Sections 951 and 2 (Count Two).

III. Discovery Provided by the Government

To date, the Government has made seven productions of Rule 16 discovery to the defense. The bulk of the Rule 16 materials were included in the Government's first productions in February and March 2022. The Government has produced over 200,000 pages of reports (some of which are redacted), thousands of hours of intercepted phone calls, thousands of electronic messages, the contents of multiple electronic accounts, consensual recordings, and other electronic surveillance.

In addition to providing the defense with these Rule 16 materials, the Government has provided a substantial volume of additional material relating to the defense's potential challenge to the Rule 41 Affidavit, including (i) information about Retired Captain-1, including his criminal history, *see* Mot. Ex. A USAO_152699-711[5]; (ii) FBI communications with and about Retired Captain-1, *see id.* USAO_152692-96; (iii) reports regarding Retired Captain-1's statements relating to this case or about his work on behalf of FBI, *see* Mot. Ex. D at 1 (referencing FBI

[5] Because Exhibit A to Girgis's Motion does not contain page numbers but encompasses multiple documents from the Government's discovery, the Government refers to the Bates numbers at the bottom of each page.

reports about Retired Captain-1, including FBI's interview of Retired Captain-1); (iv) Special Agent Connors's reports regarding and his communications with or about Retired Captain-1, *see* Mot. Ex. A USAO_152688-91; and (v) notes from the Government's interview of Special Agent Connors about his knowledge of Retired Captain-1's background, *see id.* USAO_152682-85.

DISCUSSION

I. Girgis's Motion to Compel FISA Materials and Notice for Any Additional Classified Surveillance Techniques Should Be Denied

As noted above, the Government explains the reasons requiring denial of Girgis's motion relating to FISA and other surveillance techniques in the *ex parte* Classified Supplement, a redacted unclassified version of which is attached hereto as Exhibit A, along with a declaration of the Attorney General, which is attached hereto as Exhibit B.

II. Girgis's Additional Motions to Compel Should Be Denied

Girgis also seeks to compel the production of (i) information that would be "material to Mr. Girgis's *Franks* motion"; (ii) information about "the efforts of nine Egyptian officials . . . to 'turn' expatriates into unwitting intelligence assets"; and (iii) information "about the role of" a former FBI official in the Government's investigation. Mot. at 1, 32. These motions should also be denied.

A. Applicable Law

1. Rule 16

Federal Rule of Criminal Procedure 16(a)(1)(E) provides in relevant part that the Government must, upon the defendant's request, permit the defendant to inspect or copy documents and data "if the item is within the government's possession, custody, or control" and "the item is material to preparing the defense" or "the government intends to use the item in its case-in-chief at trial." Fed. R. Crim. P. 16(a)(1)(E). To determine a defendant's right to disclosure

of particular materials, "it is necessary to decide whether those items are 'material to preparing the defense' and, if so, whether they are within the possession, custody, or control of 'the government' as that term is used in the rule." *United States v. Ghailani*, 687 F. Supp. 2d 365, 368 (S.D.N.Y. 2010). "Materiality means more than that the evidence in question bears some abstract logical relationship to the issues in the case." *United States v. Maniktala*, 934 F.2d 25, 28 (2d Cir. 1991) (citation omitted). "There must be some indication that the pretrial disclosure of the disputed evidence would [enable] the defendant significantly to alter the quantum of proof in his favor." *Id.* (citation omitted). The defendant bears the burden of establishing materiality. *Id.* (citation omitted).

2. *Brady* and *Giglio* Obligations

Pursuant to *Brady v. Maryland*, 373 U.S. 83 (1963), and its progeny, the Government has an affirmative duty to provide to the defense evidence that is favorable to the accused, known to the Government or other members of the prosecution team, and material to guilt or punishment. *See Strickler v. Greene*, 527 U.S. 263, 280-81 (1999); *Kyles v. Whitley*, 514 U.S. 419, 437 (1995). "Evidence is material only if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different." *Pennsylvania v. Ritchie*, 480 U.S. 39, 57 (1987) (internal quotation marks omitted). To demonstrate a *Brady* violation, a defendant must show that "(1) the Government, either willfully or inadvertently, suppressed evidence; (2) the evidence at issue is favorable to the defendant; and (3) the failure to disclose this evidence resulted in prejudice." *United States v. Coppa*, 267 F.3d 132, 140 (2d Cir. 2001). "*Brady* is not a rule of discovery—it is a remedial rule." *United States v. Meregildo*, 920 F. Supp. 2d 434, 440 (S.D.N.Y. 2013). Thus, "determination of a *Brady* violation is inherently a retrospective review made after a conviction or plea, and therefore, a trial court's role prior to trial

is limited." *United States v. Rodriguez*, No. 19 Cr. 779 (AKH), 2020 WL 5819503, at *10 (S.D.N.Y. Sept. 30, 2020).

B. Information Related to the Rule 41 Affidavit

Girgis indicates that he intends to file a motion seeking to suppress the warrants obtained as a result of the Rule 41 Affidavit, and seeks "further information about potential misrepresentations or omissions" in the application supporting those warrants. Mot. at 33-35. This motion should be denied as moot.

As described above, and as reflected in the exhibits attached to Girgis's Motion, the Government has made extensive disclosures related to the Rule 41 Affidavit and, in particular, about Retired Captain-1. On June 2, 2022, the Government wrote a letter to counsel for Girgis alerting the defense to the criminal history of Retired Captain-1, noting that this criminal history was not included in the Rule 41 Affidavit, and attaching notes from two interviews with Special Agent Connors conducted by the Government about Special Agent Connors's knowledge of Retired Captain-1's background. *See, e.g.*, Mot. at 2; Mot. Ex. A USAO_152682-85. In addition, in other discovery productions, as described above, the Government has produced: (i) information about Retired Captain-1, including his criminal history, *see* Mot. Ex. A USAO_152699-711; (ii) FBI communications with Retired Captain-1, *see id.* USAO_152692-96; (iii) reports regarding Retired Captain-1's statements relating to this case or about his work on behalf of FBI, *see* Mot. Ex. D at 1; and (iv) Special Agent Connors's reports regarding and his communications with or about Retired Captain-1, *see* Mot. Ex. A USAO_152688-91.

In his motion, Girgis focuses on a June 23, 2020 email sent by Special Agent Connors stating that certain government attorneys "concur[] that it does not reach the level of material misstatement/omission." Mot. at 3-4, 34; Mot. Ex. C. Girgis asserts that he needs additional

information to understand why the Government determined that any misstatement or omission in the Rule 41 Affidavit was not "material." Mot. at 34-35. As described in more detail in the Classified Supplement, Girgis appears to misapprehend this email, which does not pertain to the Rule 41 Affidavit at all.

Because the Government understands, has met, and will continue to meet its disclosure obligations surrounding any potential misstatements or omissions in the Rule 41 Affidavit, as evidenced by its June 2, 2022 letter to the defense and subsequent extensive disclosures related to Retired Captain-1 and interviews of Special Agent Connors about his knowledge of Retired Captain-1's background, Girgis's motion for additional materials related to its potential motion to challenge the Rule 41 Affidavit should be denied as moot.

C. Information About Egyptian Officials

Girgis next argues that the Government should disclose "all information regarding the efforts of [] nine Egyptians to turn expatriates into unwitting assets," including the redacted portions (to the extent they contain such information) of the FBI reports that the Government has produced relating to these officials and any other information in the Government's possession showing that those officials were involved in "a campaign to 'turn' expatriates into unwitting stooges." Mot. at 35-37. This motion too should be denied.

The Government has already provided to the defense reporting about these officials' interactions with Girgis in this case. To the extent the redacted portions of those reports contain information about these officials' interactions with other potential agents, the defense has failed to identify a basis on which such information is discoverable. The Indictment charges Girgis with acting at the direction and control of Egyptian officials and conspiring to do the same. To prove a violation of Section 951, "the Government must prove that someone 'other than a diplomatic or

consular officer or attaché' acted in the United States as an 'agent of a foreign government,' and did so without first notifying the Attorney General." *United States v. Rafiekian*, 991 F.3d 529, 542 (4th Cir. 2021) (quoting 18 U.S.C. § 951(a)). With respect to scienter, the Government must prove that the defendant (i) knowingly acted at the direction or control of a foreign official; and (ii) knew that he had not registered with the Attorney General. *See* Mot. at 37; *United States v. Duran*, 596 F.3d 1283, 1292 (11th Cir. 2010); *United States v. Alshahhi*, No. 21 Cr. 371 (BMC), 2022 WL 2239624, at *9 (E.D.N.Y. June 22, 2022), *reconsideration denied*, No. 21 Cr. 371 (BMC), 2022 WL 3595056 (E.D.N.Y. Aug. 23, 2022); *see also Alshahhi*, 2022 WL 2239624, at *9 (noting that Section 951 is a general intent crime and that it "does not also require that defendants 'specifically know that it is illegal' for them to act as agents without registering under federal law" (quoting *United States v. Bryant*, 976 F.3d 165, 172 (2d Cir. 2020))). Thus, the jury is properly tasked with determining whether *Girgis* knowingly operated on U.S. soil at the direction or control of one or more individuals that he knew to be officials of Egypt without notifying the Attorney General. Whether those same Egyptian officials were tasking others or attempting to recruit others is simply irrelevant in this case.

In addition, Girgis repeatedly describes these officials as supposedly "turning" other expatriates into "unwitting" assets or "stooges," but does not explain how that bears on any viable *mens rea* defense for Girgis in *this case*. As described above, Section 951 requires that the Government prove a defendant's knowledge that he is operating at the direction or control of a foreign government or official, and would not reach an individual who was "unwitting" of the fact that the person he was acting on behalf of was a foreign government official. Whether another uncharged individual may or may not have been a witting foreign agent within the scope of Section 951 is not relevant and discoverable in this case. Moreover, the lack of relevance is underscored

in the circumstances of this case, where there is no legitimate dispute that Girgis clearly knew he was dealing with Egyptian government officials in official positions. Girgis, for example, included the official places of employment of Ramadan and Elsayed in the contact cards for these officials in his phone: "Mohamed Ramdan Consulate" and "Mohamed Hassan Egyptian Mission," respectively. Girgis also wrote in emails seeking to set up meetings with the NYPD that he would "like to facilitate a meeting between The Administrative Control Authority of Egypt and the NYPD. The purpose is to build a bridge among both agency to better collaborate in the future." And as part of that activity, Girgis received from Mokhtar, and passed along during his efforts to set up meetings with NYPD officials, pictures of ACA officials' passports, including the passports of Mokhtar, Elbehiry, and Gamaleldim, each of which reflects that the passport holder is an ACA official. *See supra* 7. Last, Girgis discussed with Mokhtar that he acted as Mokhtar's "source," as Mokhtar berated Girgis for "insist[ing] on opening with the Mukhabarat," *i.e.*, Egypt's foreign intelligence agency. Mokhtar warned Girgis that officials in that intelligence agency "want sources for themselves, and you have become an important source for them to collect information." There is no doubt that Girgis knew the Egyptian officials with whom he interacted were exactly that—Egyptian government officials. The motion for information about purported "unwitting assets" should be denied.

D. Information About the Retired FBI Official

Finally, Girgis seeks information about the involvement of a retired FBI official (the "Official") who is under indictment on separate matters. As described below, the Official's involvement was very limited, did not include any investigative steps, and has no effect on the integrity of the investigation.

Having conducted a review of the FBI files in this case, the Government has learned that the Official's involvement was limited. Other than any involvement described in the Classified Supplement, the Official received updates from FBI investigators about the case, approved the passing of information to the NYPD, passed information sent by the NYPD to FBI agents investigating Girgis, and organized and provided a single briefing to NYPD officials regarding the case. More specifically, as reflected in discovery provided to the defense, on August 30, 2017, an FBI special agent involved in the investigation of Girgis provided a briefing to FBI leadership, including the now-retired Official, about multiple investigations, including that of Girgis. *See* USAO_155826-27. Based on these briefings, the Official organized a meeting with NYPD leadership and, on September 5, 2017, the Official and other FBI officials briefed NYPD leadership about the Girgis case. *See* USAO_155827. On October 25, 2017, the Official forwarded an email from NYPD leadership to FBI special agents involved in the investigation with the message "FYI." *See* USAO_USAO_155833-155835. And several months later, on May 10, 2018, the Official authorized the dissemination of additional information to NYPD. *See* USAO_155829.

In support of Girgis's argument that he is entitled to additional information, Girgis references allegations made against this Official in this District and in the District of Columbia. None of the facts cited by Girgis from those cases, however, supports an inference that the Official was engaged in any conduct that affected the charges here. And in any event, as noted, the Government has conducted a review of the FBI files for this case to locate any information relating to the Official. Based on the foregoing, this motion should be denied.

CONCLUSION

For the foregoing reasons, the Government respectfully requests that the Court deny Girgis's motions to compel in their entirety and without a hearing.

Dated: New York, New York
August 4, 2023

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York

By: /s/
Kyle A. Wirshba
Elinor L. Tarlow
Sarah L. Kushner
Assistant United States Attorneys
(212) 637-2493 / 1036 / 2676

Exhibit A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	)	22 Cr. 6 (KPF)
v.	)	
PIERRE GIRGIS,	)	
Defendant.	)	

THE GOVERNMENT'S ~~CLASSIFIED~~ SUPPLEMENT TO THE GOVERNMENT'S MEMORANDUM IN OPPOSITION TO THE DEFENDANT'S MOTION TO COMPEL DISCOVERY

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York

Kyle Wirshba
Elinor Tarlow
Sarah Kushner
Assistant United States Attorneys
Southern District of New York

Scott A. Claffee
Trial Attorney
National Security Division
U.S. Department of Justice

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

U.S. Constitution

Federal Statutes

Other Authorities

I. INTRODUCTION[1]

The Government submits this unclassified supplement to its memorandum in opposition to Defendant Pierre Girgis' (Girgis') Motion to Compel Discovery (ECF No. 36, hereinafter "Mot."), which requests that this Court "order disclosure of the FISA warrants, applications, and related materials, and notice of any other surveillance methods the government may have used" in its investigation of Defendant. Mot. at 31. That request for relief—addressed in Section I[2] of Girgis' Motion—would compel discovery of the Government's application(s) to the Foreign Intelligence Surveillance Court (FISC) to conduct electronic surveillance and physical search pursuant to the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801 *et seq*, and related materials filed with the FISC. By seeking such relief, Girgis has triggered FISA's provisions governing the use of FISA-obtained or -derived information in litigation, and the district court's review thereof. *See* 50 U.S.C. § 1806(c)–(h) (use and review of electronic surveillance); *id.* § 1825(d)–(i) (same for physical search).[3]

The provisions of FISA at issue are implicated when an "aggrieved person" (*i.e.*, an individual who was the target of, or subjected to, FISC-approved surveillance or search, *see* 50 U.S.C. §§ 1801(k), 1821(2)), makes "any motion or request" "to discover or obtain applications or orders or other materials relating to electronic surveillance [or physical search]," or "to discover, obtain, or suppress evidence or information obtained or derived from electronic

---

[1] A classified version of this memorandum has been filed with the Classified Information Security Officer. The pagination and footnote numbering in this unclassified memorandum differ from the classified version due to redactions.

[2] Section II of the Motion concerns non-FISA-related discovery disputes and is the subject of the Government's separate, unclassified opposition brief filed herewith.

[3] The FISA subchapter on electronic surveillance is found at 50 U.S.C. §§ 1801–1812; the subchapter on physical search, which is similarly organized and substantially identical on many points, is found at 50 U.S.C. §§ 1821–1829. This brief cites to both subchapters because the FISA-obtained or -derived information at issue relates to both electronic surveillance and physical search.

surveillance [or physical search]," *id.* §§ 1806(f), 1825(g). In that event, "if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States," the district court "shall . . . review in camera and ex parte the application, order, and such other materials relating to the surveillance [or search] as may be necessary to determine whether the surveillance [or search] of the aggrieved person was lawfully authorized and conducted." *Id.* §§ 1806(f), 1825(g). "In making this determination, the court may disclose to the aggrieved person . . . portions of the application, order, or other materials relating to the surveillance *only where such disclosure is necessary to make an accurate determination of the legality of the surveillance*." *Id.* § 1806(f) (emphasis added); *see also id.* § 1825(g) (similar). Upon determining that such surveillance and search were "lawfully authorized and conducted," the court "shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." *Id.* §§ 1806(g), 1825(h).[4]

The requisite Attorney General's affidavit is filed herewith.[5] Accordingly, the Government submits that this Court must review—*in camera* and *ex parte*—the application(s), order(s), and other materials (hereinafter, "FISA materials") relating to the electronic surveillance and physical search at issue to determine whether they were "lawfully authorized and conducted."[6] As discussed below, this Court's review will show that Girgis' request to compel discovery of "the FISA warrants, applications, and related materials" fails because (1)

---

[4] **[CLASSIFIED INFORMATION REDACTED]**

[5] As defined in FISA, "Attorney General" means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General for National Security (AAG/NS). *See* 50 U.S.C. §§ 1801(g), 1821(1). Such designation was made by then-Attorney General Eric. H. Holder, Jr., on April 24, 2009. The affidavit here, executed by AAG/NS Matthew G. Olsen, has been filed both publicly and as an exhibit within the Sealed Appendix to the classified filing. *See* Sealed Exhibit 1.

[6] **[CLASSIFIED INFORMATION REDACTED]**

such disclosure of FISA materials is unnecessary to determine the legality of the surveillance and search in this case; (2) the surveillance and search here were lawfully authorized and conducted; and (3) due process does not otherwise require disclosure of FISA materials to the Defense. Moreover, while Girgis has not yet moved to suppress any FISA information, *see* Mot. at 14 n.2, the same analysis forecloses such a suppression remedy in any event. Finally, this Court's review will show that Girgis' additional request for "notice of other surveillance methods the government may have used," including surveillance targeting non-U.S. persons[7] abroad under Section 702 of FISA, *see* 50 U.S.C. § 1881a, is without merit because the Government—in conformance with settled law—already provided Girgis the notice to which he was entitled.

A. BACKGROUND

On January 6, 2022, a grand jury in this district returned an indictment charging Girgis with acting and conspiring to act as an agent of the Arab Republic of Egypt (Egypt) without notifying the Attorney General, in violation of 18 U.S.C. §§ 371 and 951.

[CLASSIFIED INFORMATION REDACTED]

On February 15, 2022, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the Government provided notice to this Court and to Girgis of its intent to offer into evidence or otherwise use or disclose information obtained or derived from electronic surveillance and physical search conducted pursuant to FISA. *See* Dkt. No. 11.[8] On April 28, 2023, following Girgis' request that the Government permit discovery of the relevant application(s) to the FISC authorizing such surveillance and search, among other classified materials, *see* Dkt No. 32 at 1 (noting the

[7] As defined in FISA, "United States person" means (with respect to a natural person) "a citizen of the United States [or] an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of [the Immigration and Nationality Act])[.]" 50 U.S.C. § 1801(i).

[8] **[CLASSIFIED INFORMATION REDACTED]**

Government's opposition to that request), Girgis filed the instant Motion.

[CLASSIFIED INFORMATION REDACTED]

B. OVERVIEW OF THE FISA AUTHORITIES

[CLASSIFIED INFORMATION REDACTED]

1. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

2. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

3. The FISC's Findings

[CLASSIFIED INFORMATION REDACTED]

The various findings required under FISA to approve electronic surveillance or physical search, and the Government's submissions to the FISC addressing those requirements in the dockets at issue, are discussed in detail below.

II. THE FISA PROCESS

To aid this Court's review, this memorandum provides a general overview of the FISA process. Specifically, it covers the FISC's and the Attorney General's roles prescribed in FISA, the requirements for applying for a FISA order to conduct electronic surveillance or physical search, the findings the FISC must make in issuing such an order, and the procedures and standards governing a district court's review of FISA authorities when evidence obtained or derived therefrom is used in criminal proceedings. To be clear, not every part of FISA discussed below is at issue, and this memorandum generally notes where certain aspects of FISA are not directly implicated in this matter. This memorandum nevertheless discusses those other aspects in order to provide further context for this Court's review of the surveillance and search at issue.

A. OVERVIEW OF FISA

Enacted in 1978 and thereafter amended, FISA authorizes the Chief Justice of the United States to designate eleven U.S. District Judges to sit as judges of the FISC. 50 U.S.C. § 1803(a)(1). The FISC's judges have jurisdiction to review *ex parte* applications submitted by the Executive Branch for, among other authorities, authorization to conduct electronic surveillance and physical search of foreign powers and their agents within the United States. *Id.* §§ 1801(f), 1803(a)(1), 1821(5), 1822(c). The FISC's denial of such an application is subject to review by the Foreign Intelligence Surveillance Court of Review (FISC-R), an appellate panel comprised of three U.S. District or Circuit Judges designated by the Chief Justice. *Id.* § 1803(b). A FISC-R decision affirming the denial of an application is also subject to review, under the certiorari jurisdiction of the U.S. Supreme Court. *Id.*

Apart from applications to the FISC, FISA permits the Attorney General (as defined in FISA) to authorize the emergency employment of electronic surveillance or physical search for up to seven days, provided the FISC is contemporaneously notified and various other statutory requirements are satisfied. *See* 50 U.S.C. §§ 1805(e), 1824(e).[9] The government must obtain an order from the FISC approving the emergency surveillance or search if information obtained or derived therefrom is to be used in any federal or state proceeding. *See id.* Whether acquired on an emergency basis or with the FISC's approval in the ordinary course, information obtained through electronic surveillance or physical search is subject to FISA's minimization requirements, which address (among other things) the acquisition, retention, and dissemination of nonpublic information concerning unconsenting United States persons. *See id.* §§ 1801(h), 1805(e)(2), 1821(4), 1824(e)(2).

---

[9] **[CLASSIFIED INFORMATION REDACTED]**

Finally, with respect to any information that was obtained or derived from electronic surveillance or physical search conducted pursuant to FISA, such information may only be used in criminal proceedings against an aggrieved person[10] with the Attorney General's advance authorization. *See* 50 U.S.C. §§ 1806(b), 1825(c).

B. THE FISA APPLICATION

As originally enacted, FISA required a high-ranking member of the Executive Branch to certify that "the purpose" of an application to conduct electronic surveillance was to obtain foreign intelligence information; in 1994, when Congress amended FISA to allow for applications to conduct physical search, it extended the same requirement to such applications.[11] In response to the attacks of September 11, 2001, Congress modified this requirement (among other amendments to FISA) in the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). Since then, the Executive Branch official has been required to certify that obtaining foreign intelligence information is "*a significant* purpose" of the requested electronic surveillance or physical search. 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B) (emphasis added); *see also In re Sealed Case*, 310 F.3d 717, 732–36 (FISA Ct. Rev. 2002) (explaining Congress' intent in amending the certification requirement, including the "breaking down [of] barriers between criminal law enforcement and intelligence (or counterintelligence)").[12]

Foreign intelligence information is defined broadly under FISA, including "information

---

[10] For electronic surveillance, "aggrieved person" means "a person who [was] the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). For physical search, it means "a person whose premises, property, information, or material [was] the target of physical search or any other person whose premises, property, information, or material was subject to physical search." *Id.* § 1821(2).

[11] Pub. L. No. 95-511, § 104, 92 Stat. 1789 (1978) (enacting Title I, § 104(a)(7)(B) for electronic surveillance); Pub. L. No. 103-359, § 807(a)(3), 108 Stat. 3443 (1994) (enacting Title III, § 303(a)(7)(B) for physical search).

[12] Internal citations, quotations, and alternations are omitted unless noted otherwise.

that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power." 50 U.S.C. §§ 1801(e)(1), 1821(1). Foreign intelligence information also includes "information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States." *Id.* § 1801(e)(2).[13]

When the government seeks to obtain foreign intelligence information through electronic surveillance, its application to the FISC must contain, *inter alia*, the identities of the target of the surveillance and of the federal officer making the application; a statement of facts establishing probable cause to believe that the target is a foreign power or an agent of a foreign power, and that each facility or place subject to surveillance is being used, or is about to be used, by the target; a description of the types of communications or activities to be surveilled; a statement of proposed minimization procedures; a summary of the methods by which the surveillance will be conducted, including whether physical entry is required; and an official "certification" (discussed further below). 50 U.S.C. § 1804(a). An application to conduct physical search must contain the

[13] As a corollary of the requirement that obtaining foreign intelligence be "a significant purpose" of a FISA application, the FISC-R has held that an application to conduct electronic surveillance is improper if the government's "primary objective" is to gather evidence for prosecuting an ordinary "non-foreign intelligence crime," meaning a crime that is "wholly unrelated" to the offenses enumerated in 50 U.S.C. § 1801(a)–(e) (including terrorism and espionage), and that lacks any connection to such a foreign-intelligence offense. *In re Sealed Case*, 310 F.3d at 723, 736.

same or similar items, including a statement of facts justifying the applicant's belief that "the premises or property to be searched contains foreign intelligence information," and that each "premises or property to be searched is or is about to be, owned, used, possessed by, or is in transit to or from" the target. *Id.* § 1823(a).

1. Executive Branch Certification and Attorney General's Approval

Each application to conduct electronic surveillance or physical search must contain the certification of a high-ranking Executive Branch official with national security responsibilities. The contents of the certification must include:

> (A) that the certifying official deems the information sought to be foreign intelligence information;
>
> (B) that a significant purpose of the surveillance [or search] is to obtain foreign intelligence information;
>
> (C) that such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) that designates the type of foreign intelligence information being sought according to the categories described in [50 U.S.C. §] 1801(e); and
>
> (E) including a statement of the basis for the certification that –
>
> > (i) the information sought is the type of foreign intelligence information designated; and
> >
> > (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a)(6); *see also id.* § 1823(a)(6) (similar). In addition, the Attorney General must endorse the application before it is presented to the FISC, "based upon [a] finding that it satisfies the criteria and requirements" enumerated in FISA. *Id.* §§ 1804(a), 1823(a).

2. Minimization Procedures

As noted above, FISA requires that each application to conduct electronic surveillance or physical search contain "a statement of the proposed minimization procedures." 50 U.S.C. §§ 1804(a)(4), 1823(a)(4). The Attorney General has thus adopted, and the FISC has approved, minimization procedures regulating the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting United States persons obtained through surveillance or search, including persons who are not themselves the targets of FISA authorities. Among other requirements, FISA specifies that such procedures must be

> reasonably designed in light of the purpose[s] and technique of the particular surveillance [or search] to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

Id. §§ 1801(h)(1), 1821(4)(A). FISA further instructs that the minimization procedures must "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." *Id.* §§ 1801(h)(3), 1821(4)(c).

[CLASSIFIED INFORMATION REDACTED]

C. THE FISC'S ORDERS

Once an application is submitted and assigned to a judge of the FISC, it may only be approved if the FISC finds, among other things, that there is probable cause to believe that the target of the electronic surveillance or physical search is a "foreign power" or an "agent of a foreign power." 50 U.S.C. §§ 1805(a), 1824(a). Under FISA, a "foreign power" means:

> (1) a foreign government or any component thereof, whether or not recognized by the United States;
>
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or

(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

Id. §§ 1801(a), 1821(1).

With respect to an "agent of a foreign power," the definition of which varies based on whether the target is a United States person, FISA defines the term as follows:

(1) any person other than a United States person, who—
(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) [*i.e.*, an international terrorist group], irrespective of whether the person is inside the United States;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances indicate that such person may engage in such activities, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

(C) [Omitted][14]

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefor; or

---

[14] 50 U.S.C. § 1801(b)(1)(C) referred to a non-United States person who "engages in international terrorism or activities in preparation therefore [*sic*]." It was enacted in a 2004 amendment to FISA and expired on March 15, 2020. *See* Pub. L. No. 108-458, § 6001(a), 118 Stat. 3638 (2004); Pub. L. No. 116-69, § 1703, 133 Stat. 1143 (2019).

> (2) any person who—
>
> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
>
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraphs (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraphs (A), (B), or (C).

50 U.S.C. §§ 1801(b), 1821(1). In addition, FISA specifies that no United States person may be deemed a foreign power or an agent of a foreign power "solely upon the basis of activities protected by the first amendment to the [U.S.] Constitution," *id.* §§ 1805(a)(2)(A), 1824(a)(2)(A), although First Amendment-protected activity may be considered in conjunction with unprotected activity tending to show that the target is a foreign power or its agent. *United States v. Rosen*, 447 F. Supp. 2d 538, 548 (E.D. Va. 2006); *see also United States v. Rahman*, 861 F. Supp. 247, 252 (S.D.N.Y. 1994) (rejecting defendant's argument that activity arguably protected by First Amendment could not be considered in the agent-of-a-foreign-power analysis).

A FISA application must establish probable cause to believe that the target is a foreign power or an agent of a foreign power at the time of the application. *See, e.g.*, *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000); *accord United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 314 (D. Conn. 2008) ("Each application contained facts establishing probable cause to believe that, at the time the application was submitted to the FISC, the target of the FISA collection was an agent of a foreign power[.]"). However, FISA also provides that "a [FISC]

judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target," "[i]n determining whether or not probable cause exists." 50 U.S.C. §§ 1805(b), 1824(b).

Once an application has been submitted and the assigned judge makes the necessary findings (including that the application meets FISA's requirements), the FISC issues an order authorizing the electronic surveillance or physical search "as requested" in the application (or "as modified," if it concludes that a modification to the requested authorities is warranted). 50 U.S.C. §§ 1805(a), 1824(a). The FISC's order of approval must specify, *inter alia*:

> (A) the identity, if known, or a description of the specific target of the electronic surveillance [or physical search];
>
> (B) the nature and location of each facility or place at which the electronic surveillance will be directed [or of each of the premises or property to be searched];
>
> (C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance [or, for physical search, the type of information, material, or property to be seized, altered, or reproduced];
>
> (D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance [or, for physical search, a statement of the manner in which the physical search is to be conducted and, wherever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search]; and
>
> (E) the period of time during which the [surveillance or search] is approved.

Id. §§ 1805(c), 1824(c). As noted above, the duration of FISA authorities generally varies from up to 90 days, 120 days, or one year, depending on whether the target is a United States person, and whether the target is a foreign power or an agent of a foreign power, *see id.* §§ 1805(d)(1), 1824(d)(1), subject to the requirements that an authorization may not exceed "the period specified in the application" or last longer than "necessary to achieve [the] purpose" of the surveillance or search. *Id.* §§ 1805(d)(1), 1824(d)(1). FISA also authorizes the government to request extensions of surveillance and search authorities, which the FISC generally may grant

"on the same basis as an original order" (including "new findings made in the same manner as required for an original order"). *Id.* §§ 1805(d)(2), 1824(d)(2).

III. DISTRICT COURT'S REVIEW OF FISC ORDERS

FISA authorizes the use of information obtained or derived from electronic surveillance and physical search in a criminal prosecution, provided that advance authorization is obtained from the Attorney General, *see* 50 U.S.C. §§ 1806(b), 1825(c), and that notice of the surveillance and search is given to the court and to each aggrieved person against whom the information is to be used. *Id.* §§ 1806(c)–(d), 1825(d)–(e).[15] Upon receiving notice, the aggrieved person against whom FISA information is to be used may move to suppress the information on two grounds: (1) that "the information was unlawfully acquired"; or (2) that "the surveillance [or search] was not made in conformity with an order of authorization or approval." *Id.* §§ 1806(e), 1825(f).

In addition, FISA provides that a defendant who is an aggrieved person may file "a motion or request . . . pursuant to any other statute or rule of the United States . . . to discover or obtain applications or orders or other materials relating to electronic surveillance [or physical search] or to discover, obtain, or suppress evidence or information obtained or derived [therefrom]." 50 U.S.C. §§ 1806(f), 1825(g). In adjudicating such a "motion or request," if the district court "determines that the surveillance [or search] was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived [therefrom] or otherwise grant the motion of the aggrieved person." *Id.* §§ 1806(g), 1825(h). "If the court determines that the surveillance [or search] was lawfully authorized and conducted," however, "it shall deny the motion of the aggrieved person

[15] Girgis is an "aggrieved person" under FISA, and as noted above, was provided with notice of his status as such and of the Government's intent to use FISA-obtained or -derived information against him in this case.

except to the extent that due process requires discovery or disclosure." *Id.*

Here, Section I of Girgis' Motion seeks "to discover or obtain applications or orders or other materials" relating to electronic surveillance and physical search within the meaning of 50 U.S.C. §§ 1806(f) and 1825(g). *See, e.g.*, Mot. at 15. Although Girgis' Motion does not invoke 50 U.S.C. §§ 1806(e) and 1825(f) to seek suppression of FISA-obtained or -derived information, it indicates that the Defense intends to do so upon reviewing the FISA application(s) and related materials. *Id.* at 14 n.2.[16] As discussed below, however, this Court's review of the FISA materials will confirm that the surveillance and search at issue were lawfully authorized and conducted, and that due process does not otherwise require discovery or disclosure. Moreover, if Girgis were to seek suppression of evidence pursuant to 50 U.S.C. §§ 1806(e) and 1825(f), the same analysis would preclude any finding that "the information was unlawfully acquired" or that "the surveillance [or search] was not made in conformity with an order of authorization or approval." Accordingly, any request by Girgis for suppression or disclosure (whether of FISA information or FISA materials) must fail.

A. THE DISTRICT COURT'S REVIEW IS TO BE CONDUCTED *IN CAMERA* AND *EX PARTE*

Once an aggrieved person has moved for disclosure of FISA materials or suppression of FISA information, "if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States," the district court adjudicating the motion "shall, notwithstanding any other law," "review in camera and ex parte

[16] Girgis also indicates that he may seek suppression of information obtained or derived from FISA pursuant to Rule 12 of the Federal Rules of Criminal Procedure. *See id.* In all events, the judicial review provisions of 50 U.S.C. §§ 1806(f) and 1825(g) would apply to any such motion "notwithstanding any other law" due to the Attorney General's claim under oath that disclosure or an adversary hearing would harm the national security.

the application, order, and such other materials relating to the surveillance [or search] as may be necessary to determine whether the surveillance [or search] of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. §§ 1806(f), 1825(g).

[CLASSIFIED INFORMATION REDACTED]

In conducting its *in camera*, *ex parte* review, the district court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance *only where such disclosure is necessary to make an accurate determination of the legality of the surveillance* [*or search*]." 50 U.S.C. §§ 1806(f), 1825(g) (emphasis added). The district court's discretion to disclose FISA materials to an aggrieved defendant is thus highly circumscribed, and its exercise is unwarranted unless the court first concludes that it is unable to accurately determine the legality of the FISA authorities even after reviewing the Government's *in camera* and *ex parte* submissions. *See, e.g.*, *Abu-Jihaad*, 531 F. Supp. 2d at 311 ("The Court has read and re-read each [Government] submission and [FISC] order. Having done so, the Court is satisfied that disclosure and an adversary hearing are not required in this case. The Court is able to [determine] the legality of the surveillance on the basis of the materials submitted . . . *ex parte* and *in camera*."); *see also United States v. Abu-Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010) (affirming based on an independent review of the materials submitted to the district court). As the court stated in *United States v. Daoud*, "[u]nless and until a district judge performs his or her statutory duty of attempting to determine the legality of the surveillance without revealing any of the fruits of the surveillance to defense counsel, there is no basis for concluding that disclosure is necessary in order to avert an erroneous conviction." 755 F.3d 479, 484 (7th Cir. 2014).

1. *In Camera, Ex Parte* Review Is the Rule

With respect to FISA's *in camera, ex parte* review procedures, courts have "emphasized that 'disclosure and an adversary hearing are the exception occurring *only* when necessary.'" *United States v. Omar*, 786 F.3d 1104, 1110 (8th Cir. 2015) (emphasis in original) (quoting *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982)). The Second Circuit has similarly explained that "disclosure of FISA materials is the exception and *ex parte, in camera* determination is the rule." *Abu-Jihaad*, 630 F.3d at 129 (internal quotation marks and citation omitted); *accord United States v. Stewart*, 590 F.3d 93, 128 (2d Cir. 2009); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984), *superseded by statute on other grounds*, USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), *as recognized in Abu-Jihaad*, 630 F.3d at 119.[17]

With one exception, every district court to have ruled on a motion to disclose FISA materials or to suppress FISA information has determined that it was able to adjudicate the legality of the FISA collection at issue based on its *in camera, ex parte* review,[18] and every

---

[17] *Duggan* allowed that disclosure could be warranted in narrow circumstances, including "if the judge's initial review [of the government's submission] revealed potential irregularities such as 'possible misrepresentation of fact, vague identification of the persons to be surveilled[,] or surveillance records which include[] a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order.'" 743 F.2d at 78 (quoting S. Rep. No. 95-604, at 58 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3960).

[18] *See, e.g.*, *Abu-Jihaad*, 531 F. Supp. 2d at 310-11; *United States v. Al-Safoo*, 18-CR-696, 2021 WL 1750313, at *3–4 (N.D. Ill. May 4, 2021); *United States v. Kokayi*, 1:180cr-410 (LMB), 2019 WL 1186846, at *5–6 (E.D. Va. Mar. 13, 2019); *United States v. Chi Ping Ho*, 17 Cr. 779 (LAP), 2018 WL 5777025, at *5 (S.D.N.Y. Nov. 2, 2018); *United States v. Alimehmeti*, Case No. 16-398, Order Denying Motion to Suppress (Dkt. No. 67) (S.D.N.Y. Sept. 22, 2017); *United States v. Medunjanin*, No. 10 CR 19 1 (RJD), 2012 WL 526428, at *9 (E.D.N.Y. Feb. 16, 2012); *United States v. Warsame*, 547 F. Supp. 2d 982, 987 (D. Minn. 2008); *United States v. Benkahla*, 437 F. Supp. 2d 541, 554 (E.D. Va. May 17, 2006); *Rosen*, 447 F. Supp. 2d at 546; *United States v. Sattar*, No. 02 CR. 395 JGK, 2003 WL 22137012, at *6 (S.D.N.Y. Sept. 15, 2003); *United States v. Nicholson*, 955 F. Supp. 588, 592 & n.11 (E.D. Va. 1997); *United States v. Thomson*, 752 F. Supp. 75, 79 (W.D.N.Y. 1990); *United States v. Falvey*, 540 F. Supp. 1306, 1315-16 (E.D.N.Y. 1982).

appellate court to have reviewed such a determination has affirmed.[19] The one district court to have ordered disclosure of FISA materials to the defense was reversed on appeal. *See Daoud*, 755 F.3d at 484–85; *see also* 50 U.S.C. §§ 1806(h), 1825(i) (providing for interlocutory appellate review of orders granting motions to suppress FISA information or disclose FISA materials).

The materials in the Sealed Appendix confirm that there is no reason to depart from the "rule" of *in camera, ex parte* review here. This Court's review of these materials will demonstrate the FISC's proper justification for approving the authorities at issue and the Government's good-faith implementation of those authorities. This Court's review will further show the absence of any impropriety that could justify an adversary hearing or disclosure of FISA materials to the Defense. Moreover, as with the Government's previous submissions to district courts concerning FISC-approved authorities, the FISA materials here were prepared and organized to facilitate straightforward judicial review. *See, e.g.*, *In re Kevork*, 634 F. Supp. 1002, 1008 (C.D. Cal. 1985) (upholding surveillance and observing that FISA materials under review were "straightforward and readily understood"), *aff'd*, 788 F.2d 566 (9th Cir. 1986). On their face, the materials allow for an accurate judicial determination of whether the surveillance and search at issue were lawfully authorized and conducted. Indeed, as is typical in cases involving electronic surveillance and physical search conducted pursuant to FISA, "the determination of legality in this case is not complex." *Belfield*, 692 F.2d at 147; *see also Abu-Jihaad*, 531 F. Supp. 2d at 310 (similar); *Warsame*, 547 F. Supp. 2d at 987 (finding that the

---

[19] *See, e.g.*, *United States v. Turner*, 840 F.3d 336, 340 (7th Cir. 2016); *Omar*, 786 F.3d at 1110; *United States v. El-Mezain*, 664 F.3d 467, 565 (5th Cir. 2011); *United States v. Duka*, 671 F.3d 329, 338 (3d Cir. 2011); *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005); *United States v. Isa*, 923 F.2d 1300, 1306 (8th Cir. 1991)); *United States v. Hamide*, 914 F.2d 1147, 1152-53 (9th Cir. 1990). *United States v. Ott*, 827 F.2d 473, 475-76 (9th Cir. 1987); *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987); *Belfield*, 692 F.2d at 147.

"issues presented by the FISA applications are straightforward and uncontroversial"). Consistent with the approach taken by many other courts, this Court can review the FISA materials *in camera* and *ex parte* and make the requisite legal determinations without the need for an adversary hearing or disclosure of classified materials to the Defense.

Apart from the specific harms that would result from disclosing the FISA materials in this case, as detailed in the Declaration and Claim of Privilege of the AAG/NS and supporting declaration, the underlying rationale for non-disclosure is clear. "Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to *anyone* not involved in [a] surveillance operation." *Ott*, 827 F.2d at 477 (emphasis in original); *accord Medunjanin*, 2012 WL 526428, at *9 (finding that "unsealing the FISA materials . . . would provide the defense with unnecessary details of an extraordinarily sensitive anti-terrorism investigation"). In particular, the importance of protecting sensitive intelligence sources cannot be overstated. If such sources believe that the United States "will be unable to maintain the confidentiality of its relationship to them, many [of those sources] could well refuse to supply information." *CIA v. Sims*, 471 U.S. 159, 175 (1985).

When considering whether the disclosure of classified sources, methods, techniques, or other information would harm the national security, courts have generally refrained from superseding the judgments of Executive Branch officials responsible for determining whether a particular disclosure would present an unacceptable risk of compromising intelligence-gathering processes. Among other issues, such judgments include consideration of whether certain information, which may not appear sensitive on its own, could be pieced together with a mosaic of other information (both public and non-public) to permit adversaries to glean insights enabling

them to defeat U.S. counterintelligence efforts. *See, e.g.*, *Sims*, 471 U.S. at 179–80 ("The Director reasonably concluded that an observer who is knowledgeable about a particular intelligence research project . . . could, upon learning that research was performed at a certain institution, . . . deduce the identities of the individual researchers who are protected 'intelligence sources.'"); *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods."). That consideration further underscores how disclosing FISA materials or conducting an adversary hearing is not only unnecessary to adjudicate Girgis' Motion, but could also result in heightened risks to national security that courts have consistently sought to avoid.

Indeed, Congress enacted FISA's *in camera*, *ex parte* review procedures to account for such risks in accommodating the judiciary's need to review any FISA authorities that may be implicated in litigation against aggrieved persons. As the D.C. Circuit explained in *Belfield*:

> Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights. In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law-enforcement surveillance.

692 F.2d at 148 (internal quotation marks and citations omitted); *accord Daoud*, 755 F.3d at 483 ("[FISA] is an attempt to strike a balance between the interest in full openness of legal proceedings and the interest in national security, which requires a degree of secrecy concerning the government's efforts to protect the nation.").

2. *In Camera, Ex Parte* Review Is Constitutional

Since FISA's enactment, litigants have challenged the constitutionality of its *in camera, ex parte* review procedures on various grounds. For example, the defendants in *United States v. Dhirane* "argue[d] that it was contrary to our constitutionally established adversary system to deny their counsel, who possessed the requisite security clearance, access to the [FISA] applications and supporting materials," and that FISA's procedures prevented them from vindicating their right to a *Franks* hearing. *See* 896 F.3d 295, 299 (4th Cir. 2018); *see also Franks v. Delaware*, 438 U.S. 154 (1978) (recognizing the right to an adversarial hearing on the validity of a warrant upon a preliminary showing of an intentional or reckless falsehood in the warrant affidavit). In rejecting these arguments, the court explained:

> The government notes that every federal court to have considered the constitutionality of these procedures has concluded that FISA reached a reasonable and therefore constitutional balance of competing interests. [Collecting cases.] And we share that view. It is consistent with the general notion, even in the criminal context, that the right to an adversarial proceeding to determine disputes of fact is not absolute.

Dhirane, 896 F.3d at 300 (citing in part *Kaley v. United States*, 571 U.S. 320, 338 (2014), and *Taglianetti v. United States*, 394 U.S. 316, 317 (1969)). Like those other courts, the Second Circuit has repeatedly upheld the constitutionality of FISA's *in camera, ex parte* review provisions. *See Stewart*, 590 F.3d at 126 (concluding that "the procedures fashioned in FISA [are] a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information" (quoting *Duggan*, 743 F.2d at 73)); *Abu-Jihaad*, 630 F.3d at 117.

In sum, because the AAG/NS has stated under oath that disclosing or conducting an adversary hearing with respect to the FISA materials would harm national security, Girgis' Motion must be adjudicated using FISA's review procedures. Those procedures are

constitutional and impose a general "rule" of *in camera, ex parte* review. There is no basis to depart from that rule in this case, and this Court should accordingly review the FISA materials *in camera* and *ex parte* when determining whether the electronic surveillance and physical search at issue were "lawfully authorized and conducted." 50 U.S.C. §§ 1806(g), 1825(h).

B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

An application to conduct electronic surveillance or physical search under FISA is "subject to 'minimal scrutiny by the courts,' both upon initial presentation [to the FISC] and subsequent challenge [before a district court]." *Abu-Jihaad*, 630 F.3d at 130 (quoting *Duggan*, 743 F.2d at 77). "[A]bsent a showing sufficient to trigger a *Franks* hearing," "'the representations and certifications submitted in support of an application for FISA surveillance should be presumed valid' by a reviewing court." *Id.* (quoting *Duggan*, 743 F.2d at 77 n.6). "Of course, even minimal scrutiny is not toothless." *Id.* In assessing whether evidence was lawfully collected from FISC-approved surveillance or search, "a reviewing district court must consider: (1) whether the certification by the Executive Branch in support of the FISA application was properly made; (2) whether the application established probable cause; and (3) whether the collection followed proper minimization procedures." *United States v. Liu*, 19-CR-804 (VEC) 2021 WL 6127396, at *1 (S.D.N.Y. Dec. 28, 2021) (citing *Abu-Jihaad*, 630 F.3d at 130–31); *see also Chi Ping Ho*, 2018 WL 5777025, at *5 (articulating same three-part test). The discussion immediately below addresses the standards of review applicable to this Court's assessment of the FISC's probable cause findings and the Executive Branch certification(s) at issue. The standards governing this Court's assessment of compliance with proper minimization procedures are addressed in Section IV.C of this memorandum.

1. Standard of Review for the FISC's Probable Cause Findings

Courts have not definitively resolved whether the FISC's probable cause findings should be reviewed *de novo* or deferentially.[20] In the Second Circuit, district courts "tend to give the FISC's [probable cause] determination due deference." *Liu*, 2021 WL 6127396, at *1; *see also Abu-Jihaad*, 630 F.3d at 130 (observing that the "standard of judicial review applicable to FISA warrants is deferential," although "the government's detailed and complete submissions . . . would easily allow it to clear a higher standard of review"); *United States v. Fishenko*, No. 12 CV 626 (SJ), 2014 WL 4804215, at *3–5 (E.D.N.Y. Sept. 25, 2014) (similar); *Medunjanin*, 2012 WL 526428, at *6-7 (affording deferential review, while observing this "does not mean that such review is superficial"). In any event, the FISA materials here demonstrate that the FISC's probable cause determinations readily satisfy even a *de novo* standard of review.

2. Probable Cause Under FISA

For the FISC to approve electronic surveillance or physical search, FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power, and that each facility or place at which the surveillance is directed is being used, or is about to be used, by a foreign power or an agent thereof (or, for physical search, that the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from, a foreign power or an agent thereof). 50 U.S.C. §§ 1805(a), 1824(a). It is this standard—not the standard applicable to a criminal search warrant—that this Court must apply. *See Abu-Jihaad*, 630 F.3d at 130–31; *see also Omar*, 786 F.3d at 1111 ("[R]ather than focusing on probable cause

---

[20] *Compare, e.g.*, *Turner*, 840 F.3d at 340 (applying *de novo* review), *with United States v. Ahmed*, No. 1:06-CR-147-WSD-GGB, 2009 U.S. Dist. Lexis 120007, at *21 (N.D. Ga. Mar. 19, 2009) (concluding that the FISC's "determination of probable cause should be given 'great deference' by the reviewing court").

to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power." (quoting *El-Mezain*, 664 F.3d at 564)).

[CLASSIFIED INFORMATION REDACTED]

The Second Circuit has repeatedly affirmed the constitutionality of FISA's probable cause requirements under the Fourth Amendment, both before and after the USA PATRIOT Act modified FISA in 2001, confirming that obtaining foreign-intelligence information need only be "a significant purpose" (as opposed to *the primary* purpose) of the electronic surveillance or physical search. *See Abu-Jihaad*, 630 F.3d at 120.[21] *Abu-Jihaad*'s analysis of this issue relied to a significant extent on the Supreme Court's decision in *United States v. U.S. District Court (Keith)*, 407 U.S. 297 (1972). There, in considering the Fourth Amendment's warrant requirement and the standards for conducting traditional law enforcement wiretapping under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (hereinafter, "Title III"), the Court indicated that the Fourth Amendment would countenance different standards for a warrant to conduct domestic security surveillance. *See id.* at 321–22. With particular relevance here, *Keith* reasoned (1) that "the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency"; (2) that the "focus of . . . surveillance [in domestic security investigations] may be less precise than that directed against more conventional types of crime"; (3) that unlike ordinary criminal investigations, "[t]he gathering of security intelligence is often long range and

[21] Numerous other courts have also affirmed the constitutionality of FISA's probable cause requirements. *See Abu-Jihaad*, 630 F.3d at 120 (collecting more than a dozen cases). The one decision holding otherwise—*i.e.*, that FISA's probable cause standard, in light of the USA PATRIOT Act's "significant purpose" modification, violates the Fourth Amendment—was vacated on standing grounds. *Mayfield v. United States*, 504 F. Supp. 2d 1023 (D. Or. 2007), *vacated*, 599 F.3d 964, 973 (9th Cir. 2010).

involves the interrelation of various sources and types of information"; and (4) that the "exact targets of such surveillance may be more difficult to identify" than in surveillance targeting ordinary criminals. *Id.* *Keith* was decided before FISA's enactment and only addressed *domestic* security surveillance. *See id.* at 321–22 (expressly reserving judgment on the issue of warrantless surveillance directed at the "activities of foreign powers or their agents"). However, as the Second Circuit has recognized, *Keith*'s rationale applies *a fortiori* to foreign intelligence surveillance, where the Government's interests would generally be even more compelling. *See Abu-Jihaad*, 630 F.3d at 122 (observing that *Keith*'s considerations "supporting different warrant standards [for domestic intelligence] pertain equally to foreign intelligence surveillance.").[22]

3. Standard of Review for Executive Branch Certifications

The certification that FISA requires for an application to conduct electronic surveillance or physical search is "subject to only minimal scrutiny by the courts" and "presumed valid." *Duggan*, 743 F.2d at 77 & n.6. In particular, "[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Id.* When an aggrieved person challenges FISC-approved surveillance or search before the district court, the "reviewing court is to have no greater authority to second-guess the executive branch's certifications than has the FISA Judge." *Id.*; *see also Chi Ping Ho*, 2018 WL 5777025, at *5 (same).

For a FISA application targeting a non-United States person, "[t]he FISA Judge need only determine that the application contains all of the statements and certifications required by

[22] FISA's procedures were enacted partly in response to *Keith*, and numerous courts have recognized that those procedures satisfy the Fourth Amendment's requirement of reasonableness, in view of the reasoning from *Keith* discussed above. *See, e.g.*, *Duggan*, 743 F.2d at 74; *In re Sealed Case*, 310 F.3d at 738, 746; *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987).

[FISA]." *Duggan*, 743 F.2d at 75. When a United States person is targeted, the FISC must also find that the certifications are "not clearly erroneous." *Id.* (citing 50 U.S.C. § 1805(a)). A "clearly erroneous" finding is established only when, "although there is evidence to support it, the reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed." *United States v. Islamic American Relief Agency*, No. 07-0087-CR-W-NKL, 2009 WL 5169536, at *4 (W.D. Mo. Dec. 21, 2009) (assessing certifications for applications targeting United States persons) (quoting *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948)).[23]

4. The "Good Faith" Exception Applies to FISA

Even if a district court were to determine that a particular application to the FISC failed to satisfy FISA's requirements, any evidence obtained or derived from FISC-approved electronic surveillance or physical search would nonetheless be admissible under the "good faith" exception to the exclusionary rule, recognized in *United States v. Leon*, 468 U.S. 897 (1984). Courts have found that *Leon*'s good-faith exception would apply to FISA-acquired evidence. *See, e.g.*, *United States v. Ning Wen*, 477 F.3d 896, 898 (7th Cir. 2007); *Ahmed*, 2009 U.S. Dist. Lexis 120007, at *25 n.8. Moreover, there is no indication here that the FISC failed to act in a neutral and detached manner, or that any assertion in a FISA application was deliberately or recklessly false, as might warrant exclusion of evidence obtained pursuant to a FISC order of approval. *See Leon*, 468 U.S. at 926. To the contrary, this Court's review of the FISA materials will confirm that the officials who applied for and implemented the FISA authorities at issue did so in good faith, and that the Government reasonably relied on the FISC's order(s) of approval in conducting electronic surveillance and physical search. Therefore, although Girgis has yet to

[23] **[CLASSIFIED INFORMATION REDACTED]**

move for suppression of FISA-obtained or -derived evidence, any attempt to do so would fail (at a minimum) under *Leon*'s good-faith exception.

IV. THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH AT ISSUE WERE LAWFULLY AUTHORIZED AND CONDUCTED

This section first discusses the materials in the Sealed Appendix in order to demonstrate, in light of the standards of review described above, that the FISA authorities in this matter were lawfully *authorized*. This section then addresses the Government's good-faith compliance with proper minimization procedures and related requirements in order to demonstrate that the electronic surveillance and physical search at issue were lawfully *conducted*.

A. THE INSTANT FISA APPLICATION(S) SATISFIED FISA'S PROBABLE CAUSE STANDARDS

[CLASSIFIED INFORMATION REDACTED]

1. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

2. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

a. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

b. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

c. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

3. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

a. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

b. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

c. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

d. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

4. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

a. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

b. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

B. THE CERTIFICATION(S) COMPLIED WITH FISA

[CLASSIFIED INFORMATION REDACTED]

1. Foreign Intelligence Information

[CLASSIFIED INFORMATION REDACTED]

2. "A Significant Purpose"

[CLASSIFIED INFORMATION REDACTED]

3. Information Not Reasonably Obtainable Through Normal Investigative Techniques

[CLASSIFIED INFORMATION REDACTED]

C. THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH WERE CONDUCTED IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

[CLASSIFIED INFORMATION REDACTED]

1. The Minimization Procedures

Once a reviewing district court is satisfied that FISA information was lawfully *acquired*, it must then examine whether the electronic surveillance and physical search at issue were lawfully *conducted*. *See* 50 U.S.C. §§ 1806(e)(2), 1825(g). To do so, the reviewing court must determine whether the government followed the relevant minimization procedures to appropriately minimize the information acquired pursuant to FISA.

[CLASSIFIED INFORMATION REDACTED]

FISA's legislative history and applicable case law demonstrate that the definitions of "minimization procedures" and "foreign intelligence information" were intended to take into account the realities of collecting foreign intelligence, including that the activities of those engaged in clandestine intelligence gathering or international terrorism are often not obvious on their face. *See Rahman*, 861 F. Supp. at 252–53. The degree to which information is required to be minimized may vary given the specifics of a particular investigation, such that less minimization at acquisition is justified when "the investigation is focusing on what is thought to be a widespread conspiracy" and more extensive surveillance is necessary "to determine the precise scope of the enterprise." *In re Sealed Case*, 310 F.3d at 741; *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 286 (S.D.N.Y. 2000) (agreeing with the government that "more extensive monitoring and greater leeway in minimization efforts are permitted in a case like this given the world-wide, covert and diffuse nature of the international terrorist group(s) targeted"). Furthermore, the activities of foreign powers and their agents are often not obvious from an

initial or cursory overhear of conversations. To the contrary, agents of foreign powers frequently engage in coded communications, compartmentalized operations, the use of false identities, and other practices designed to conceal the breadth and aim of their operations, organization, activities and plans. *See, e.g., United States v. Salameh*, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two conspirators involved in the 1993 bombing of the World Trade Center in New York referred to the bomb plot as the "study" and to terrorist materials as "university papers"). As one court explained, "[i]nnocuous-sounding conversations may in fact be signals of important activity; information on its face innocent when analyzed or considered with other information may become critical." *In re Kevork*, 634 F. Supp. at 1017 (quoting H.R. Rep. No. 95-1283, pt. 1, at 55 (1978)); *see also In re Sealed Case*, 310 F.3d at 740–41 (comparing minimization under FISA and Title III); *Thomson*, 752 F. Supp. at 81 (noting that it is permissible to retain and disseminate "bits and pieces" of information until the information's "full significance becomes apparent") (citing H.R. Rep. No. 95-1283, pt. 1, at 58).

Likewise, "individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time." *Rahman*, 861 F. Supp. at 252–53 (citing H.R. Rep. No. 95-1283, pt. 1, at 55, 59). In addition, the government may require greater flexibility in the FISA context due to the likelihood that some communications involving foreign agents will be carried out in a foreign language (as happened here). *See, e.g.*, *United States v. Mubayyid*, 521 F. Supp. 2d 125, 134 (D. Mass. 2007) (upholding ten-year period for retention of FISA-acquired communications, including because the communications were in a foreign language). At bottom, "courts have construed 'foreign intelligence information' broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information." *Rosen*, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also impacts implementation of the minimization procedures at the retention and dissemination stages. There is a legitimate need to conduct a thorough post-acquisition review of FISA information that involves a United States person who is acting as an agent of a foreign power. As Congress explained:

> It is "necessary" to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

H.R. Rep. No. 95-1283, pt. 1, at 58. Indeed, as one court cautioned, when a United States person communicates with an agent of a foreign power, the government would be "remiss in meeting its foreign counterintelligence responsibilities" if it did not thoroughly "investigate such contacts and gather information to determine the nature of those activities." *Thomson*, 752 F. Supp. at 82. In light of these realities, Congress recognized that "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." *See* S. Rep. No. 95-701, at 39 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4008.

Accordingly, in reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with respect to particular communications. To the contrary, courts have emphasized the statement in FISA's legislative history that "[a]bsent a charge that the minimization procedures have been disregarded completely, the test of compliance is whether a good faith effort to minimize was attempted." *Mubayyid*, 521 F. Supp. 2d at 135 (quoting S. Rep. No. 95-701, at 39–40 (1978)); *see also Scott v. United States*, 436 U.S. 128, 136 (1978) (holding, in the context of Title III minimization, that there should be an "objective assessment of the [agents'] actions in light of

the facts and circumstances confronting [them] at the time"). Courts have accordingly assessed compliance with FISA minimization requirements under a "rule of reason," *see, e.g.*, *Chi Ping Ho*, 2018 WL 5777025, at *7, with the understanding that "Congress did not intend for nominal failure to abide the minimization procedures to undercut entire investigations," *United States v. Aziz*, 228 F. Supp. 3d 363, 378 (M.D. Pa. 2017).

Moreover, FISA expressly provides that the government is not required to minimize information that is "evidence of a crime," even if it is not foreign intelligence information. 50 U.S.C. §§ 1801(h)(3), 1821(4)(c). As a result, to the extent that certain communications of a United States person may be evidence of a crime or otherwise may establish an element of a substantive or conspiratorial offense, such communications need not be minimized. *See, e.g.*, *Chi Ping Ho*, 2018 WL 5777025, at *6.

Even if certain communications were not minimized in accordance with the SMPs, suppression would not be the appropriate remedy with respect to those communications that met the standard. As discussed above, absent evidence that there has been a complete disregard for the minimization procedures, the fact that some communications should have been minimized does not affect the admissibility of others that were properly acquired and retained. FISA's legislative history indicates that Congress intended only a limited sanction for errors of minimization:

> As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

H.R. Rep. No. 95-1283, pt. 1, at 93; *see also Medunjanin*, 2012 WL 526428, at *12 (disclosure and suppression not warranted where "failure to adhere to [the minimization] protocol was *de minimis*"); *Liu*, 2021 WL 6127396, at *3 (similar); *Chi Ping Ho*, 2018 WL 5777025, at *7

("Although the Government acknowledged that in 'limited occasions described herein, certain communications were not properly minimized,' the Court finds that the Government's failure . . . in these instances was *de minimis* and that on the whole the agents have shown a high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion" (internal quotation marks and citations omitted)).

2. The FISA Information Was Appropriately Minimized

[CLASSIFIED INFORMATION REDACTED]

Based upon this information, the Government submits that it lawfully conducted the FISA collection discussed herein. Consequently, for the reasons stated above, this Court should find that the FISA collection at issue was lawfully conducted under proper minimization procedures.

D. DUE PROCESS DOES NOT REQUIRE DISCOVERY OR DISCLOSURE

As noted earlier, FISA provides that once a district court has concluded that electronic surveillance and physical search were "lawfully authorized and conducted," "it shall deny the motion of the aggrieved person *except to the extent that due process requires discovery or disclosure*." 50 U.S.C. §§ 1806(g), 1825(h) (emphasis added). Girgis references these FISA provisions and due process more generally to argue that he is entitled to discovery of the FISA materials, *see, e.g.*, Mot. at 12, 16, 21–22, 27, but his arguments are unavailing. The Second Circuit has rejected the notion that FISA's review procedures are unconstitutional because "due process require[s] that [a defendant] have access to . . . FISA applications and warrants." *Stewart*, 590 F.3d at 126. Moreover, Girgis cannot identify any due process violation arising from the application of FISA's review procedures in this case, nor does one appear from reviewing the FISA materials at issue. *See Abu-Jihaad*, 630 F.3d at 129 (concluding, from an

independent review of the classified record, that the district court appropriately found no denial of due process in barring discovery or an adversary hearing with respect to FISA materials); *Chi Ping Ho*, 2018 WL 5777025, at *5 ("FISA's *in camera* and *ex parte* review provisions comport with the Constitution's due process requirements. The constitutionality of these provisions has been affirmed by every federal court that has considered the matter, including the Court of Appeals."); *United States v. Hasbajrami*, No. 11-cr-623 (DLI), 2017 WL 3610595, at *4 (E.D.N.Y. Apr. 6, 2017) ("In analyzing FISA, the 'Second Circuit has made clear that proceeding *ex parte* does not, standing alone, offend notions of fundamental fairness.'" (quoting *Medunjanin*, 2012 WL 526428, at *9)).[24]

The plain intention of 50 U.S.C. §§ 1806(g) and 1825(h)—allowing this Court to order disclosure of material to which the defendant would be entitled under the Due Process Clause, such as material that had not been previously disclosed under *Brady v. Maryland*, 373 U.S. 83 (1963), even while ruling against the defendant's motion generally—cannot be interpreted to

[24] Defense counsel notes that he holds a security clearance and has experience dealing with classified discovery. *See* Mot. at 23 n.4. As discussed above, the only statutory authorities that grant a court discretion to disclose the FISA materials at this stage are set out at 50 U.S.C. §§ 1806(f) and 1825(g), and these provisions permit disclosure only where the court finds that it is unable to determine the legality of the electronic surveillance and physical search based on its *in camera*, *ex parte* review alone and without the assistance of defense counsel. Defense counsel's security clearance does not affect the need to have an *ex parte*, *in camera* review to determine whether disclosure would harm national security. *See Daoud*, 755 F.3d at 481-86; *see also Abu-Jihaad*, 630 F.3d at 129; *Medunjanin*, 2012 WL 526428, at *9 ("Defense counsel's security clearances add little to the case for disclosure."). While holding a valid security clearance is a necessary prerequisite to reviewing classified information, it is not a sufficient basis for a court to order disclosure of classified information to defense counsel. Counsel may access classified information only if they hold both the required clearance and a "need-to-know" the information, *Hasbajrami*, 2017 WL 3610595, at *6, and cleared counsel only has a "need to know" if the court determining the legality of the surveillance concludes that disclosure is "necessary," *Daoud*, 755 F.3d at 484; *accord Rosen*, 477 F. Supp. 2d at 546. If this Court concludes from its *in camera*, *ex parte* review of the FISA materials that it is capable of accurately determining the legality of the FISA collection at issue, then no defense attorney, even one with an otherwise appropriate security clearance, would have a "need to know" any of the FISA materials. There is nothing extraordinary about this case to justify an order to disclose the highly sensitive and classified FISA materials under the applicable FISA standard.

support Girgis' demand for access to all of the FISA materials in advance of this Court's *in camera, ex parte* review and determination of the legality of the collection. The necessity of disclosing FISA materials is a factual, not a legal, question. With respect to any claim that the FISA materials contain information that due process requires be disclosed to the Defense, the request is premature since this Court will make that factual determination for itself during its *in camera, ex parte* review. The Government is confident that this Court's review of the challenged FISA materials will not reveal any material that due process requires be disclosed to Girgis, such as *Brady* material, as provided for in 50 U.S.C. §§ 1806(g) and 1825(h). Accordingly, the provisions concerning due process in 50 U.S.C. §§ 1806(g) and 1825(h) cannot justify disclosure of, or an adversary hearing with respect to, the FISA materials at issue.

V. GIRGIS' ADDITIONAL ARGUMENTS FOR DISCLOSURE ARE WITHOUT MERIT

The discussion above demonstrates that the electronic surveillance and physical search at issue were lawfully authorized and conducted; that due process does not otherwise require discovery or disclosure; and, therefore, that Girgis' Motion must fail to the extent it seeks to "order disclosure of the FISA warrants, applications, and related materials." Mot. at 31. Nonetheless, for the sake of completeness, this section addresses the specific arguments raised in Section I of the Motion relating to the FISC-approved authorities under review. In addition, this section addresses' Girgis' request in Section I for this Court to order "notice of any other surveillance methods the government may have used" in its investigation of him. *Id.*

A. *FRANKS v. DELAWARE* DOES NOT REQUIRE DISCLOSURE

Girgis has not moved for a hearing pursuant to *Franks*, 438 U.S. 154. Instead, Girgis notes that "[t]he defense anticipates raising a *Franks* claim with regard to the FISA motions" in his case, and that disclosure of the FISA materials "is necessary so the defense can meaningfully

litigate an apparent *Franks* issue." Mot. at 13-14. To merit a *Franks* hearing, a defendant must make a "substantial preliminary showing" that the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit, and that the resulting misrepresentation was essential to the finding of probable cause. *Franks*, 438 U.S. at 155–56. As this Court's review of the FISA materials will demonstrate, no material false statements or omissions exist with respect to the information the Government is using against Girgis. Moreover, for the reasons discussed below, this Court should decline Girgis' suggestion to order the disclosure of the FISA materials so that Girgis can pursue a *Franks* hearing.

As stated above, to obtain a hearing, *Franks* requires a defendant to make a "concrete and substantial preliminary showing" that the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit, and that the resulting misrepresentation was essential to the finding of probable cause. *Franks*, 438 U.S. at 155–56. Courts apply the same standard when a defendant seeks a *Franks* hearing as part of a challenge to FISA collection. *See Duggan*, 743 F.2d at 77 n.6; *see also Liu*, 2021 WL 6127396, at *3 (applying the *Franks* standard in a case involving FISA materials). A defendant must show that the affiant agent lied or recklessly disregarded the truth with specific evidence in the form of "[a]ffidavits or sworn or otherwise reliable statements of witnesses." *Franks*, 438 U.S. at 171. The *Franks* threshold is not met even by an offer of proof of an impropriety that might have affected the outcome of the probable cause determination, but rather requires one that was "necessary to the finding of probable cause." *United States v. Colkley*, 899 F.2d 297, 301-02 (4th Cir. 1990); *see also United States v. Shnewer*, No. 07-459, 2008 U.S. Dis. LEXIS 112001, at *38 (D.N.J. Aug. 17, 2008) ("[E]ven if the Court were to determine there existed a reckless or intentional falsehood or omission in the FISA application materials, the evidence obtained still

should not be suppressed unless the Court makes the further finding that the falsehood or omission was material to the probable cause determination.").

Only after Girgis makes the requisite showing may this Court conduct a *Franks* hearing to determine if there are material misrepresentations of fact, or omissions of material fact, in the FISA applications sufficient to warrant suppression of the FISA-obtained or-derived evidence.[25] *See Franks*, 438 U.S. at 171. Under the relevant case law, "[w]ithout such a showing, he is foreclosed from obtaining a hearing." *United States v. Kashmiri*, No. 09 CR 830-4, 2010 WL 4705159, at *6 (N.D. Ill. Nov. 10, 2010).[26] But Girgis ignores this burden and speculates that "material misstatements in the traditional search warrant application strongly indicates the existence of a *Franks* claim as to the FISA warrant applications." Mot. at 15.

[CLASSIFIED INFORMATION REDACTED]

Second, citing prior instances of purported government misrepresentations or omissions in other cases or contexts does not satisfy the *Franks* standard, "as it sheds no light on the truth or falsity of the particular FISA application under review." *Daoud*, 755 F.3d at 492 (Rovner, J. concurring). If this were determined to be sufficient, then Girgis, and defendants in every case, would be permitted to obtain the FISA materials by merely referencing other irrelevant impropriety. Disclosing FISA materials to defendants would then become the rule, violating Congress' clear intention, set forth in 50 U.S.C. §§ 1806(f) and 1825(g), that the FISA materials

---

[25] Indeed, even if a defendant offers sufficient proof to show that an affidavit involved false statements or omissions, a hearing should not be held if the affidavit would still provide probable cause if the allegedly false material were eliminated, or if the allegedly omitted information were included. *See Franks*, 438 U.S. at 171; *Colkley*, 899 F.2d at 300; *United States v. Ketzeback*, 358 F.3d 987, 990 (8th Cir. 2004); *United States v. Martin*, 615 F.2d 318, 328 (5th Cir. 1980).

[26] Judge Rovner's concurring opinion in *Daoud*, cited by the defense (*see* Mot. at 16-17), does not mandate a contrary conclusion. Judge Rovner joined the unanimous panel opinion "in full," 755 F.3d at 485, and made clear that a potential *Franks* claim is not an automatic basis for disclosure of the classified FISA materials. *Id.* at 494-95.

be reviewed *in camera* and *ex parte* in a manner consistent with the realities of intelligence needs and investigative techniques.

While many courts have acknowledged the difficulty for defendants to meet this burden in cases in which information obtained or derived from FISA is being used against them, they agree that the *Franks* evidentiary burden still must be met. *See Daoud*, 755 F.3d at 483-84 ("Defense counsel would like to mount [a *Franks*] challenge in this case. But that's hard to do without access to the classified materials. . . . The drafters [of FISA] devised a solution: the judge makes the additional determination, based on full access to all classified materials and defense's proffer of its version of events, of whether it's possible to determine the validity of the *Franks* challenge without disclosure of any of the classified materials to the defense."); *Belfield*, 692 F.2d at 148 ("Congress was also aware of these difficulties [faced by defense counsel without access to FISA materials and] chose to resolve them through means other than mandatory disclosure."); *see also United States v. Alwan*, No. 1:11-CR-13-R, 2012 WL 399154, at *8-10 (W.D. Ky. Feb. 7, 2012) ("The Court is cognizant of the substantial difficulties [the defendant] has encountered in trying to assert a *Franks* violation. Regardless of the difficulties, however, it does not change the evidentiary burdens he must meet.").[27]

Courts have rejected other defendants' attempts to force a *Franks* hearing by positing unsupported speculation to challenge the validity of FISC orders, and this Court should do so here. *See Turner*, 840 F.3d at 341-42 (in reviewing the classified and unclassified record, the

[27] Girgis argues generally that he is constitutionally entitled to effectively vindicate his right to a *Franks* hearing, particularly given the "volume of information at issue," but FISA's *in camera*, *ex parte* review procedures prevent him from doing so, in violation of both FISA and the Due Process Clause. *See* Mot. at 15–16. However, as noted above, courts have declined to find any violation of the Constitution with respect to a defendant's purported inability to effectively challenge FISA authorities under *Franks*, and courts have uniformly upheld FISA's *ex parte*, *in camera* review procedures. *See supra* Sections III.A.1-2, IV.D; *see also Dhirane*, 896 F.3d at 300 (collecting cases).

Court found that it made "a meaningful effort to confirm the accuracy of the [FISA] application") (quoting *Daoud*, 755 F.3d at 494-95 (Rovner, J. concurring) (characterizing this review as serving "the same interest . . . that a *Franks* motion serves"); *see also Kashmiri*, 2010 WL 4705159, at *6 (noting that the court "has already undertaken a process akin to a *Franks* hearing through its *ex parte*, *in camera* review"); *Shnewer*, 2008 U.S. Dist. LEXIS 112001, at *37 ("This catch-22 has not troubled courts, however, and they defer to FISA's statutory scheme."); *Abu-Jihaad*, 531 F. Supp. 2d at 309; *Mubayyid*, 521 F. Supp. 2d at 131 ("The balance struck under FISA – which is intended to permit the gathering of foreign intelligence under conditions of strict secrecy, while providing for judicial review and other appropriate safeguards – would be substantially undermined if criminal defendants were granted a right of disclosure simply to ensure against the possibility of a *Franks* violation.").

Here, Girgis failed to carry the burden of establishing the prerequisites for an adversarial hearing, and his attempt to obtain disclosure of the FISA materials to meet that burden runs counter to FISA, *Franks*, precedent, and the intent of Congress. For these reasons, this Court should reject Girgis' argument that disclosure of the FISA materials is necessary so that he can pursue a *Franks* hearing. Moreover, this Court's *in camera*, *ex parte* review of the FISA materials will demonstrate that "an adversary hearing in this case would be academic because there is no question the FISA applications pass muster." *Medunjanin*, 2012 WL 526428, at *9.

B. GIRGIS' REMAINING ARGUMENTS FOR DISCLOSURE OF THE FISA MATERIALS ARE UNAVAILING

Girgis' remaining arguments in support of compelling production of FISA materials fare no better. Girgis argues that "[d]isclosure is necessary for the defense to litigate the other FISA-related suppression issues presented in this case." *See* Mot. at 17–20. Here, Girgis speculatively challenges the FISC's determinations (a) that Girgis was an agent of a foreign power; (b) the

official certification that foreign intelligence information sought under FISA could not reasonably be obtained through normal investigative procedures; and (c) the official certification that collection of foreign intelligence information was at least a "significant purpose" of the applications. In addition, Girgis challenges (d) the Government's adherence to minimization requirements, and (e) the duration of FISA electronic surveillance and physical search. *See id.*

[CLASSIFIED INFORMATION REDACTED]

Girgis also claims, in support of disclosure to challenge whether he was an agent of a foreign power, that the Defense "cannot meaningfully litigate" the "difficult issue" of whether Girgis was targeted solely on the basis of First Amendment-protected activity without disclosure of the FISA materials. Mot. at 17-18. While the Government does not publicly identify the targets of the FISA applications at issue, Girgis characterizes the Government's allegations of his activities to "turn entirely on his alleged attempts to organize large trips to Egypt and arrange meetings of various kinds, distribute information, express support for certain groups, and converse with various individuals." *Id.* at 18. Girgis assumes that the FISA applications rely solely on First Amendment-protected activity and, in describing Girgis' activities, fail to recognize that not all speech or advocacy-related activities fall within the protection of the First Amendment. For instance, conversations with co-conspirators merit no First Amendment protection. *See Rahman*, 189 F.3d at 117 ("[I]f the evidence shows that the speech[] crossed the line into criminal solicitation, procurement of criminal activity, or conspiracy to violate the laws, the prosecution is permissible."); *see also United States v. Sattar*, 395 F. Supp. 2d 79, 101 (S.D.N.Y. Oct. 24, 2005) ("The First Amendment lends no protection to participation in a conspiracy, even if such participation is through speech"). Moreover, even activities that clearly fall within the purview of the First Amendment's protection may be considered by the FISC if

other activity is indicative that the target is an agent of a foreign power. *See Turner*, 840 F.3d at 353; *Rosen*, 447 F. Supp. 2d at 549-50.

[CLASSIFIED INFORMATION REDACTED]

Finally, Girgis argues that "FISA is unconstitutional as applied to this case" to the extent "that FISA's statutory rules bar disclosure" of FISA materials that could affect a suppression ruling. *See* Mot. at 21–24. This argument fails under the weight of authority discussed above. Numerous cases (including from the Second Circuit) have considered the same or similar arguments, all of which were found to be unavailing. *See supra* Section III.A (collecting authorities); *see also, e.g.*, *Stewart*, 590 F.3d at 126 (rejecting constitutional challenge to FISA's *ex parte*, *in camera* review procedures).

C. THIS COURT SHOULD LIKEWISE DENY GIRGIS' MOTION FOR NOTICE REGARDING ANY OTHER SURVEILLANCE METHODS

Girgis' motion also seeks an order compelling notice regarding surveillance methods used, "including surveillance under Executive Order 12,333, FISA Section 702, or national security letters." *See* Mot. at 24-25. Specifically, Girgis moves this Court to order the Government to "disclose whether it intends to use information obtained or derived from these or any other surreptitious surveillance methods against Mr. Girgis." *Id.* at 26-27. In making this request, Girgis cites the Fourth Amendment to the Constitution, 18 U.S.C. § 3504, and Federal Rule of Criminal Procedure 16 (hereinafter, "Rule 16"). *Id.* at 27-30. As this Court will note from its *in camera*, *ex parte* review of the FISA materials, and for the reasons stated below, the Government has complied with its notice and discovery obligations, and thus, Girgis' motion lacks merit and should be denied.

The government's discovery obligations in a criminal case are not limitless. *See United States v. Agurs*, 427 U.S. 97, 106 (1976) (the government is under "no duty to provide defense counsel with unlimited discovery of everything known by the prosecutor"); *United States v. Phillips*, 854 F.2d 273, 277 (7th Cir. 1988) (finding that discovery rules do "not grant criminal defendants unfettered access to government files"); *United States v. Griebel*, 312 F. App'x 93, 96 (10th Cir. 2008) (the government's discovery obligations "are defined by Rule 16, *Brady*, *Giglio*, and the Jencks Act"); *United States v. Colon*, No. 97 CR 659, 1998 WL 214714, at *7-9 (N.D. Ill. Apr. 21, 1998) (addressing the government's discovery obligations). Further, there is no rule of discovery that requires the government to provide a defendant with a clear, concise narrative regarding the origins of the criminal investigation that led to his arrest. *See Pennsylvania v. Ritchie*, 480 U.S. 39, 59 (1987) ("defendant's right to discover exculpatory evidence does not include the unsupervised authority to search through the [government's] files"); *United States v. Bagley*, 473 U.S. 667, 675 (1985) ("the prosecutor is not required to deliver his entire file to defense counsel"). Rather, the government is required to provide the defense with all discoverable material (including exculpatory information) described in Rule 16.

Notice concerning the government's intent to use evidence in a criminal case is generally governed by Federal Rules of Criminal Procedure 12 and 16. Rule 12(b)(4)(B) provides, in relevant part:

> [T]he defendant may, in order to have an opportunity to move to suppress evidence under Rule 12(b)(3)(C), request notice of the government's intent to use (in its evidence-in-chief at trial) any evidence that the defendant may be entitled to discover under Rule 16.

The purpose of this rule is to "provide the defendant with sufficient information to file the necessary suppression motions." *United States v. Ishak*, 277 F.R.D. 156, 158 (E.D. Va. 2011) (internal quotation marks and citation omitted). "Thus, the government's obligation under Rule

12(b)(4)(B) ends when it has made disclosures that sufficiently allow the defendant to make informed decisions whether to file one or more motions to suppress." *Id.* The Government has satisfied this obligation and provided Girgis with sufficient information and notice to file any necessary motions to suppress. No court has interpreted Rule 12(b)(4)(B) to require the government to give an accounting of every investigative technique used in the case, regardless of its relationship to admissible evidence. Girgis' request for more information than is legally required should be denied.

[CLASSIFIED INFORMATION REDACTED]

In the context of FISA collection, Congress decided to allow for greater protection of information than is normally afforded because of the need to protect sensitive national security information, which includes classified sources and methods. Congress intended that FISA "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." S. REP. NO. 95-701, at 16, 1978 U.S.C.C.A.N., at 3985. As such, in recognition of "the nature of the national interests implicated in matters involving a foreign power or its agents," Congress provided for more limited disclosure than is ordinarily provided with regard to criminal defense. *Belfield*, 692 F.2d at 148.

Girgis' contention that he is entitled to enhanced notice is further refuted by Congress's assignment of broader FISA notice requirements in certain circumstances, not to include in the context of criminal defendants. *See Dean v. United States*, 556 U.S. 568, 573 (2009) ("[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."). Specifically, Congress identified three scenarios where more

specific notice regarding FISA surveillance was warranted. *See* 50 U.S.C. § 1806(j) (notice of particular information regarding surveillance required where the Attorney General approves emergency surveillance and the government does not later obtain authorization from the FISC); *id.* § 1825(b) (requiring notice identifying property seized, altered, or reproduced during physical search of a U.S. person's residence where the Attorney General has determined that there is no national security interest in continued secrecy); *id.* § 1825(j) (notice of particular information regarding physical search required where the Attorney General approves emergency physical search and the government does not later obtain authorization from the FISC).[28] Congress elected not to require such broad disclosure in the situation where a defendant is charged in a criminal proceeding. *See id.* §§ 1806(c) and 1825(d) (requiring only notice "that the United States intends" to use or disclose FISA-obtained or -derived information).

Nevertheless, Girgis argues that he is entitled to additional notice and discovery under 18 U.S.C. § 3504. Mot. at 28-30. That section provides, in relevant part:

> In any trial, hearing, or other proceeding in or before any court . . . [u]pon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an unlawful act or because it was obtained by the exploitation of an unlawful act, the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act.

Importantly, 18 U.S.C. § 3504 is not applicable in the instant matter because no "unlawful act" has occurred. 18 U.S.C. § 3504(a)(1) and (b). The FISA-obtained or -derived evidence was not the product of an unlawful act; to the contrary, it was lawfully obtained pursuant to orders of the FISA. Moreover, the Government provided the notice required under the FISA statute (50 U.S.C. §§ 1806(c) and 1825(d)). No court has held that in addition to 50 U.S.C. §§ 1806(c) or

---

[28] **[CLASSIFIED INFORMATION REDACTED]**

1825(d), the government has an additional notice requirement under 18 U.S.C. § 3504.

A specific statutory provision normally controls over one of more general application. *See Bloate v. United States*, 559 U.S. 196, 207-08 (2010); *Gozlon-Peretz v. United States*, 498 U.S. 395, 407 (1991). Moreover, 50 U.S.C. §§ 1806(c) and 1825(d) were enacted in 1978 and 1994, respectively, approximately eight and 24 years after 18 U.S.C. § 3504 was adopted in 1970. *See* Organized Crime Control Act of 1970, Pub. L. No. 91-452, § 702, 84 State. 922, 935-36 (1970). "[A] later enacted statute may limit the scope of an earlier statute." *Bhd. of Maintenance of Way Emps. v. CSX Transp., Inc.*, 478 F.3d 814, 817 (7th Cir. 2007); *see also Ku v. U.S. Dep't of Housing and Urban Dev.*, No. 11 CV 6858(VB), 2012 WL 2864509, at *4 (May 14, 2012) ("[A] later enacted statute may limit the scope of an earlier enacted statute to the extent they conflict.") (citing *In re Ionosphere Clubs, Inc.*, 922 F.2d 984, 991 (2d Cir. 1990)). Thus, there is no basis for holding that 18 U.S.C. § 3504 trumps FISA's "later-enacted, more specific" notice provisions. Finally, Girgis failed to establish a colorable basis to believe that he has been aggrieved by unlawful surveillance of any kind.

For the foregoing reasons, this Court should deny Girgis' motion for notice and discovery.

D. GIRGIS HAS NOT ESTABLISHED ANY BASIS FOR THIS COURT TO SUPPRESS THE FISA INFORMATION

As noted earlier, Girgis' Motion does not include any request to suppress evidence obtained or derived from FISC-approved electronic surveillance or physical search. Mot. at 14 n.2. Girgis states that this is because he must first review the FISA materials to determine what grounds there are for suppression, indicating that he intends to file a motion to suppress FISA-obtained or -derived evidence at a later date. *See* Mot. at 10. Regardless, any request by Girgis to suppress FISA information would fail under the analysis set forth in this memorandum.

Because the surveillance and search at issue were "lawfully authorized and conducted" for purposes of 50 U.S.C. §§ 1806(g) and 1825(h), Girgis cannot obtain a suppression remedy pursuant to those provisions. *See id.* ("If the court determines that the surveillance [or search] was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure."). Furthermore, Girgis cannot obtain the suppression remedy afforded by 50 U.S.C. §§ 1806(e) and 1825(f). Those provisions only permit suppression of FISA-obtained or -derived evidence when (1) the "information was unlawfully acquired," or (2) the underlying "surveillance [or search] was not made in conformity with an order of authorization of approval," *id.*, and both prongs are unavailing when the surveillance and search were "lawfully authorized and conducted." *See, e.g.*, *Al-Safoo*, 2021 WL 1750313, at *3–4 (adjudicating defendant's motion for disclosure of FISA materials and separate motion for suppression of FISA information and concluding, based on same analysis, that the FISA collection at issue was both "lawfully conducted" and "made in conformity with an order of authorization or approval"). For the reasons discussed above and briefly recounted below, no suppression of FISA-obtained or -derived evidence could be warranted in this case.

1. The Government Has Satisfied the Certification, Significant Purpose, and Normal Investigative Techniques Standards

[CLASSIFIED INFORMATION REDACTED]

As part of the USA PATRIOT Act, Congress amended FISA to require that an Executive Branch official now certify that "a significant purpose" of the requested surveillance was to obtain foreign intelligence information. 18 U.S.C. § 1804(a)(6)(B). The "significant purpose" standard has been repeatedly upheld, including by the Second Circuit. As the Second Circuit observed in *Abu-Jihaad*, "we identify no constitutional infirmity in Congress's decision to allow FISA warrants to issue on certification of a 'significant purpose' to obtain foreign intelligence

information. . . ." 630 F.3d at 131; *see also id.* at 128 (concluding that the standard "is sufficient to ensure that the executive may only use FISA to obtain a warrant when it is in good faith pursuing foreign intelligence gathering. . . ."); *Duka*, 671 F.3d at 343 ("the dispositive issue is whether the 'significant purpose' test is reasonable. . . . We agree with our sister courts of appeals and the Foreign Intelligence Surveillance Court of Review that the amended FISA's 'significant purpose' standard is reasonable under the Fourth Amendment.").

[CLASSIFIED INFORMATION REDACTED]

2. The Government Has Satisfied the Probable Cause Standard

[CLASSIFIED INFORMATION REDACTED]

As discussed above in § III.B , the probable cause threshold that the Government must satisfy before receiving authorization to conduct electronic surveillance and physical search under FISA complies with the Fourth Amendment's reasonableness standard. Arguments that FISA's different probable cause standard violates the Fourth Amendment have been uniformly rejected by federal courts. *See, e.g., Abu-Jihaad,* 630 F.3d at 120 (listing sixteen cases that have ruled FISA does not violate the Fourth Amendment).

3. The Government Complied with the Minimization Procedures

FISA requires that the Government comply with all applicable procedures to appropriately minimize information acquired pursuant to FISA. *See* 50 U.S.C. § 1805(a)(3).

[CLASSIFIED INFORMATION REDACTED]

VI. CONCLUSION: THERE IS NO BASIS FOR THIS COURT TO DISCLOSE THE FISA MATERIALS OR SUPPRESS THE FISA INFORMATION

Based on the analysis above, the Government submits that this Court must conduct an *in camera, ex parte* review of the FISA materials and the Government's classified submission. The

Government further submits that, following such review, this Court should: (1) hold that disclosure of the FISA materials and the Government's classified submission or any portions thereof to Girgis, or conducting an adversary hearing with regard to those materials, is improper because this Court can determine the legality of the electronic surveillance and physical search at issue without such disclosure; (2) find that the FISA surveillance and search in this matter were lawfully authorized and conducted; and (3) accordingly deny Girgis' Motion to the extent it seeks disclosure of FISA materials. In addition, in the event that this Court believes the issue of whether to suppress the fruits of FISC-approved electronic surveillance or physical search is ripe for decision—whether based on the parties' briefing on the instant Motion, or based on another motion by Girgis that expressly seeks such suppression—the Government requests that this Court (4) hold that such a suppression remedy should be denied. Separately, with respect to Girgis' request for an order providing "notice of other surveillance methods the government may have used" in investigating him, the Government requests that this Court (5) hold that Girgis is not entitled to further notice and accordingly deny such relief. Finally, the Government requests that this Court (6) order that the FISA materials and the Government's classified submissions be maintained under seal by the Classified Information Security Officer or his or her designee.

As noted earlier, district court orders (1) granting a motion or request under 50 U.S.C. §§ 1806(g) or 1825(h), or (2) finding that an electronic surveillance or physical search was not lawfully authorized or conducted, or (3) requiring the disclosure of FISA materials are final orders for purposes of appeal. *See* 50 U.S.C. §§ 1806(h), 1825(i). Should this Court conclude that any disclosure of FISA materials or FISA information is warranted, or that any FISA-obtained or -derived information must be suppressed, the Government, given the significant national security consequences involved, would likely pursue an appeal. Accordingly, the

Government requests that this Court stay any such order pending an appeal by the United States of that order.

Dated: August 4, 2023

Respectfully Submitted,

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York

By: /s/
Kyle Wirshba
Elinor Tarlow
Sarah Kushner
Assistant U.S. Attorneys

Scott Claffee
Trial Attorney
National Security Division

Exhibit B

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	)	22 Cr. 6 (KPF)
v.	)	
PIERRE GIRGIS,	)	
Defendant.	)	

DECLARATION AND CLAIM OF PRIVILEGE OF THE ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY

I, Matthew G. Olsen, hereby declare the following:

1. I am the Assistant Attorney General for National Security and an officer of the United States Department of Justice, an Executive Department of the United States. I have official custody of and control over the relevant files and records of the United States Department of Justice. The matters stated herein are based on my knowledge, on consideration of information available to me in my official capacity as the Assistant Attorney General for National Security, on discussions that I have had with other Department of Justice officials, and on conclusions I have reached after my review of this information.

2. Under the authority of 50 U.S.C. §§ 1806(f) and 1825(g), I submit this declaration pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, in connection with the above-captioned criminal proceeding.[1] I have been advised that the Government presently intends to use information obtained or derived from FISA-authorized electronic

[1] As defined in FISA, "Attorney General" means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon designation of the Attorney General, the Assistant Attorney General for National Security. *See* 50 U.S.C. §§ 1801(g), 1821(1). Such designation was made by then-Attorney General Eric H. Holder, Jr., on April 24, 2009.

surveillance and physical search in the criminal proceedings against the Defendant, Pierre Girgis. *See* 50 U.S.C. §§ 1806(c), 1825(d). I understand that the Defendant was provided notice of the Government's intent to use FISA information and that the Defendant, by and through his attorney, has filed a motion seeking disclosure of the application(s) submitted to, and the order(s) issued by, the Foreign Intelligence Surveillance Court, as well as other related materials (hereinafter collectively referred to as the "FISA Materials"), in anticipation of later seeking to suppress information obtained or derived pursuant to FISA (hereinafter, the "Defendant's Motion"). The Government is opposing the Defendant's Motion. For the reasons set forth in the Government's opposition, it is necessary to provide this Court with the FISA Materials.

3. Based on the facts and considerations set forth below, I hereby claim that it would harm the national security of the United States to disclose or hold an adversary hearing with respect to the FISA Materials. *See* 50 U.S.C. §§ 1806(f), 1825(g). The United States will be submitting the relevant classified documents to this Court as part of a Sealed Appendix, so this Court may conduct an *in camera*, *ex parte* review of the FISA Materials. My Claim of Privilege also extends to the classified portions of any memoranda, briefs, or other documents the Government may file in connection with this litigation and to any oral representations that may be made by the Government that reference the classified information contained in the FISA Materials.

4. In support of my Claim of Privilege, the United States is submitting to the Court for *in camera*, *ex parte* review the Declaration of Suzanne Turner, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation. The Declaration of Assistant Director Turner sets forth in detail the specific facts on which my Claim of Privilege is based. The Declaration of Assistant Director Turner is classified at the "TOP SECRET" level. The FISA Materials are classified at the "TOP SECRET" and "SECRET" levels.

5. Relying on the facts set forth in the Declaration of Assistant Director Turner, I certify that the unauthorized disclosure of the FISA Materials that are classified at the "TOP SECRET" level reasonably could be expected to cause exceptionally grave damage to the national security of the United States. I further certify that the unauthorized disclosure of the FISA Materials that are classified at the "SECRET" level reasonably could be expected to cause serious damage to the national security of the United States. The FISA Materials contain sensitive and classified information concerning United States intelligence sources and methods and other information related to efforts of the United States to conduct counterintelligence investigations, including the manner and means by which those investigations are conducted. As a result, the unauthorized disclosure of the information could harm the national security interests of the United States.

6. I respectfully request that the Court treat the contents of the Sealed Appendix, for security purposes, in the same sensitive manner that the contents were treated in the submission to this Court, and to return the Sealed Appendix to the Department of Justice upon the disposition of the Defendant's Motion. The Department of Justice will retain the Sealed Appendix under the seal of the Court subject to any further orders of this Court or other courts of competent jurisdiction.

Pursuant to Title 28, United States Code, Section 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 3rd day of July, 2023.

Matthew G. Olsen
Assistant Attorney General for National Security